07/2022

10 lat EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Europejski Miesiąc Cyberbezpieczeństwa

„Zwolnij” i „Pomyśl”, czyli jak bronić się przed socjotechnikami hakerów?

Przestępczość gospodarcza - zagrożenie stabilności firmy

Co biznes musi wiedzieć o procesach krytycznych?

Komunikacja w czasie cyberataku

Globalny problem z MFA

SPIS TREŚCI

SZANOWNI PAŃSTWO,

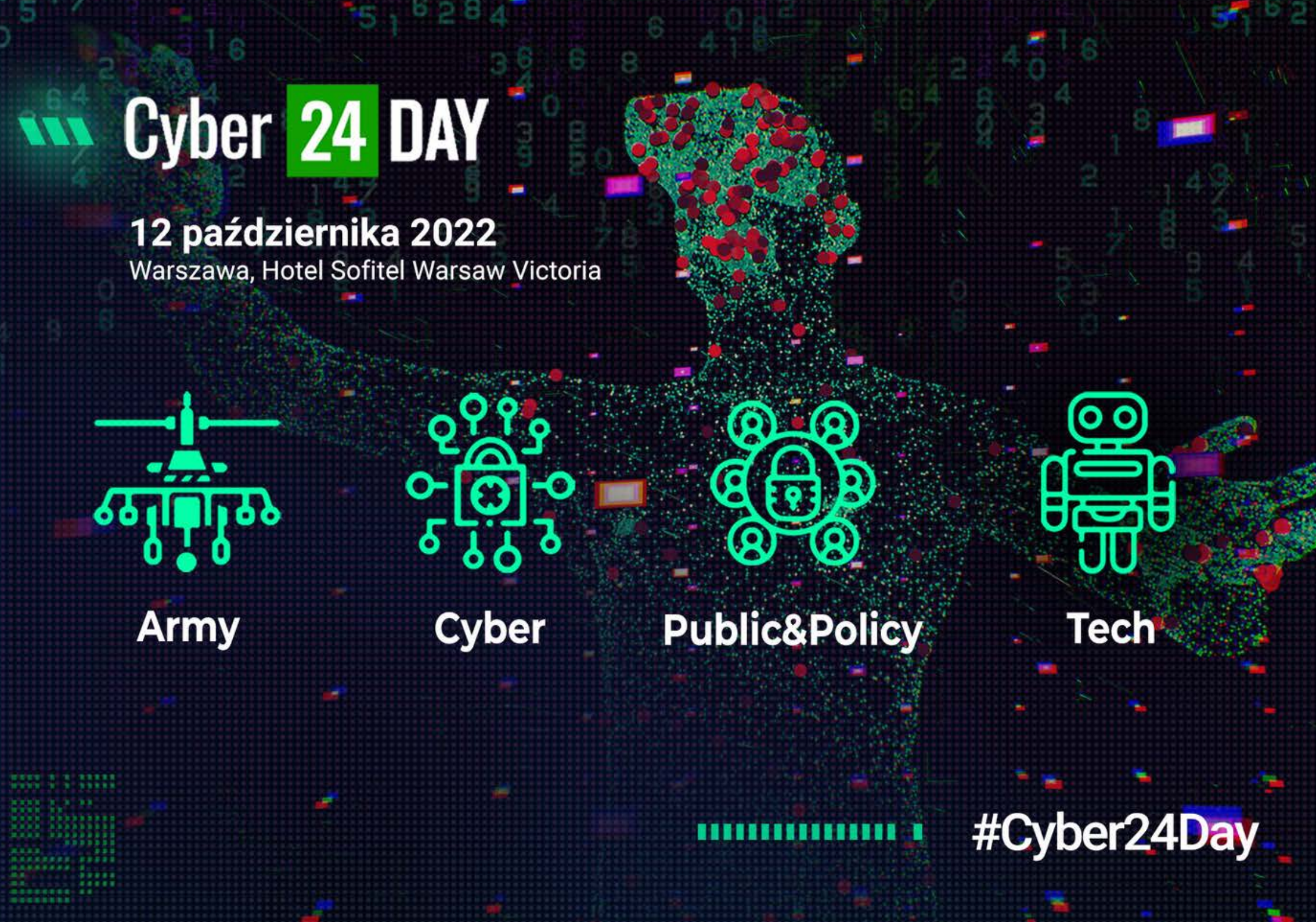
wydanie, które macie przed swoimi oczami jest wyjątkowe z kilku względów. Mamy październik - Europejski Miesiąc Cyberbezpieczeństwa.

Z tej okazji NASK zakwalifikował "Security Magazine" jako ogólnoeuropejską inicjatywę, która ma na celu edukować i uświadamiać Polaków, jak ważne jest cyberbezpieczeństwo. Dzięki wsparciu merytorycznemu NASK przez cały miesiąc będziemy pokazywać naszym czytelnikom i obserwatorom, jak - zwłaszcza teraz - istotne jest przeciwdziałanie, ochrona i łagodzenie skutków cyberataków - zwłaszcza przez firmy.

Na łamach naszego październikowego wydania pojawiły się: fotorelacja z patronowanej przez nas we wrześniu imprezy, a także zaproszenia na kolejne jakże ważne konferencje poświęcone bezpieczeństwu naszego kraju, bezpieczeństwu IT, bezpieczeństwu lokalnemu oraz startupom.

Wszystkich zainteresowanych promocją swojego wydarzenia związanego z security zachęcamy do kontaktu i współpracy.

Rafał Stępniewski


Cyber 24 DAY
12 października 2022
Warszawa, Hotel Sofitel Warsaw Victoria
Army
Cyber
Public&Policy
Tech
#Cyber24Day

PATRONAT
SECURITY MAGAZINE

KLUCZOWE DYSKUSJE WOKÓŁ CYBERBEZPIECZEŃSTWA

KONFERENCJA CYBER24DAY 12 PAŹDZIERNIKA

Rejestracja jest nadal możliwa dla przedstawicieli branży TUTAJ (po zaakceptowaniu udziału przez organizatora) oraz dla mediów. Szczegóły wydarzenia znajdują się na stronie: www.cyber24day.pl

Część debat będzie transmitowana w serwisie YouTube i na stronie organizatora: www.cyberdefence24.pl

Konferencja Cyber24 Day, organizowana przez Grupę Defence24, to jedno z najważniejszych forum na mapie wydarzeń, które skupiają się na tematyce cyberbezpieczeństwa, cyfryzacji i nowych technologii. 12 października 2022 roku odbędzie się już III edycja, podczas której przedstawiciele rządu, administracji, pracownicy cywilni, wojskowi i eksperci będą dyskutowali na bieżące tematy. Wciąż można się zarejestrować.

Cyber24 Day ma na celu stworzenie forum do dyskusji na kluczowe tematy w branży cyberbezpieczeństwa, by decydenci, reprezentujący administrację publiczną i Siły Zbrojne RP mogli wziąć udział w debatach, mających wpływ na przyszłe decyzje polityczne, a eksperci i media znaleźli przestrzeń do pogłębiania wiedzy oraz rozmów z liderami z sektora technologicznego i obronnego z całego świata.

Panele, debaty i prezentacje z udziałem polskich i zagranicznych gości będą skupiały się na tematyce cyberobrony w aspekcie wojskowym i cywilnym, prywatności danych, roli dyplomacji w branży cyberbezpieczeństwa, sztucznej inteligencji czy suwerenności w kontekście gospodarki cyfrowej.

Jednym z punktów programu będzie przemówienie Serhii Demediuka, zastępcy sekretarza Rady Bezpieczeństwa Narodowego i Obrony Ukrainy. Opowie o sytuacji w cyberprzestrzeni w czasie rosyjskiej inwazji na Ukrainę.

Konferencja jest objęta Patronatami Honorowymi: Janusza Cieszyńskiego, Sekretarza Stanu ds. Cyfryzacji w Kancelarii Prezesa Rady Ministrów, Ministerstwa Obrony Narodowej, Ministerstwa Spraw Zagranicznych oraz Biura Bezpieczeństwa Narodowego. Partnerzy główni wydarzenia to Microsoft oraz Samsung.

Konferencja odbędzie się 12.10 w Warszawie, w Hotelu Sofitel Warsaw Victoria.

PAŹDZIERNIK: EUROPEJSKI MIESIĄC CYBERBEZPIECZEŃSTWA

Rafał Stępniewski
Rzetelna Grupa

10 lat EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

W tym roku obchodzimy po raz 10. Europejski Miesiąc Cyberbezpieczeństwa. Tegoroczna edycja ma dwa główne motywy przewodnie. Są nimi phishing oraz ransomware. Nie bez powodu wybrano takie zagadnienia. Są to najczęstsze metody wykorzystywane obecnie przez cyberprzestępców, mające na celu bezpośrednie lub pośrednie wykorzystanie swoich ofiar do wyłudzenia i kradzieży pieniędzy.

W samym 2021 roku CERT Polska zarejestrował ponad 116 tys. różnego rodzaju zgłoszeń, gdzie phishing stanowił ok. 76% z nich. Względem roku 2020 zanotowano wzrost o 196%.

W samej Polsce w roku 2021 roku było ponad 22 tys. różnych ataków phishingowych skierowanych zarówno do firm, jak i konsumentów - uśredniając ponad 60 dziennie.

W Polsce koordynatorem całej akcji edukacyjnej jest NASK. Przez 31 dni października różne organizacje zarówno publiczne, jak i firmy prywatne mogą przeprowadzać inicjatywy i wydarzenia, których celem jest edukacja w zakresie bezpiecznego korzystania z nowych technologii i internetu.

Grupą docelową, do jakiej może być adresowane wydarzenie, są zarówno osoby dorosłe z rozróżnieniem na seniorów, jak i dzieci i młodzież.

Głównym celem jest realizacja misji edukacyjnej, ale dla firm komercyjnych jest to wspaniała możliwość budowy wizerunku oraz bezpłatnej promocji oferowanych produktów, rozwiązań i usług. Co ważne, firmy mogą organizować wydarzenia na poziomie krajowym, ale również europejskim, otrzymując bezpłatną promocję oraz rozgłos.

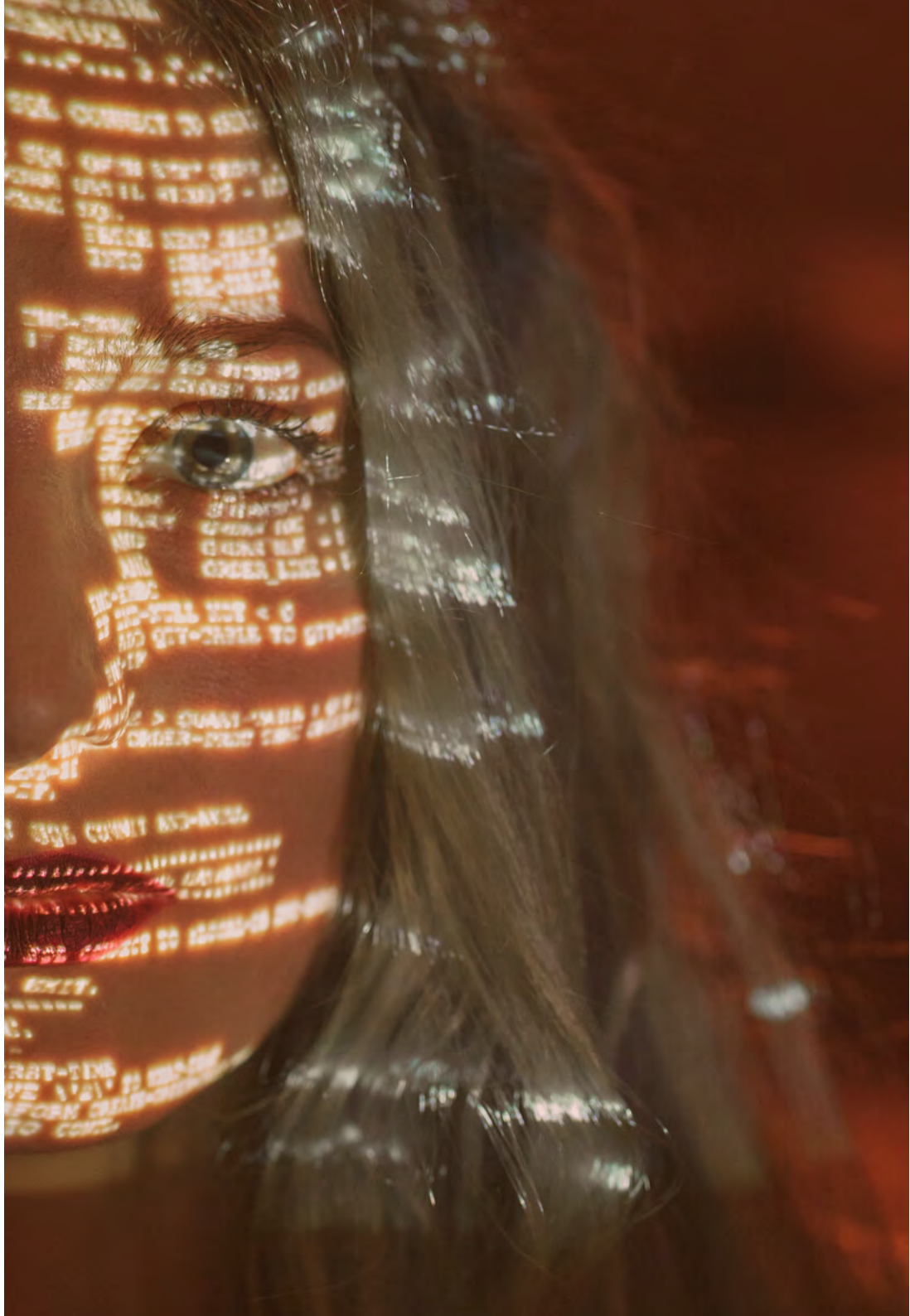
W szczególności wydarzenie może być przeznaczone dla właścicieli firm lub pracowników tychże firm, ale również dla konsumentów.

Oczywiście, organizując wydarzenie należy pamiętać o tym, że edukacja i budowanie świadomości jest najważniejsze - promocja uslug i produktów powinna być na drugim planie i może stanowić uzupełnienie poruszanego zagadnienia.

Wydarzeniem może być konferencja, webinar, szkolenie zarówno stacjonarne jak i online, ale też prowadzenie kampanii edukacyjnych w mediach społecznościowych. Można również zorganizować grę lub zawody. Jest to kilka przykładów form wydarzeń, a jeżeli firma bądź organizacja ma swój pomysł wpisujący się w ideę akcji bez wątpienia będzie mogła zgłosić taką inicjatywę.

Już dziś zgłoszono niemal 200 różnych wydarzeń i inicjatyw na poziomie Europy, a niemal połowa z nich ma mieć miejsce w Niemczech. Ich liczba świadczyć może o dużej świadomości problemu, jakim jest edukacja w zakresie cyberbezpieczeństwa.

By dołączyć do akcji, należy zaplanować w październiku organizację wydarzenia, związanego



z bezpieczeństwem i za pośrednictwem STRONY wysłać swoje zgłoszenie.

Bez wątpienia cała akcja ma szczytny cel. Obecnie życie bez technologii jest niemal niemożliwe, więc świadomość zagrożeń, jakie mogą nas spotkać w cyfrowym świecie, jest bardzo ważna. Nie każdy ma wiedzę techniczną i doświadczenie, a cyberprzestępcy wykorzystują naiwność, nieuwagę, a czasem i naturalną chęć skorzystania z okazji, żeby nie powiedzieć chciwość.

Tym samym, miło mi poinformować, że również redakcja **"Security Magazine" dołączyła do ogólnoeuropejskiej kampanii ECSM 2022, którą w Polsce koordynuje NASK**, włączając nasze wydania do inicjatywy na rzecz edukacji w zakresie cyberbezpieczeństwa

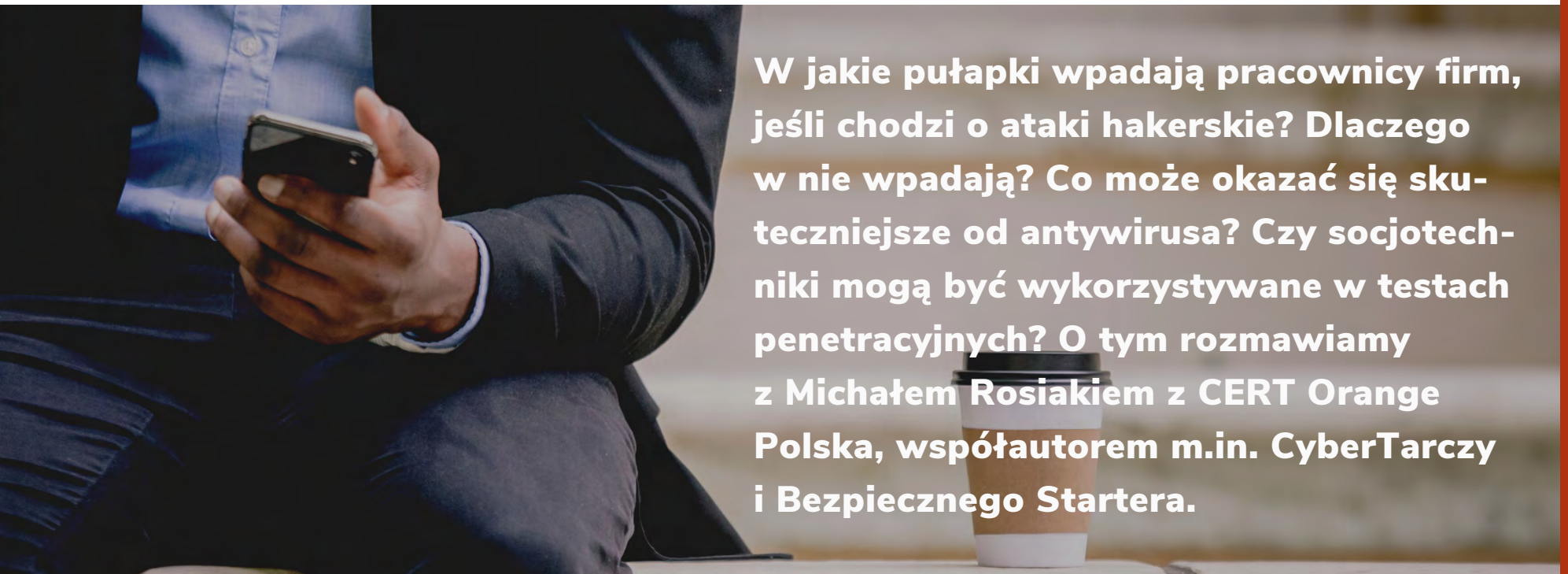
Również przez cały październik będziemy prowadzić na naszych kanałach w mediach społecznościowych cykl poświęcony Europejskiemu Miesiącowi Cyberbezpieczeństwa.

Zapraszam na nasze kanały: LINKEDIN i FACEBOOK.


ZAPISZ SIĘ NA
NEWSLETTER
BY NIE PRZEOCZYĆ
KOLEJNEGO WYDANIA
SECURITY MAGAZINE
Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy
SECURITY MAGAZINE
ZAPISZ SIĘ
NEWSLETTER
YOUR EMAIL HERE
SUBSCRIBE

„ZWOLNIJ” I „POMYŚL”, CZYLI JAK BRONIĆ SIĘ PRZED SOCJO-TECHNIKAMI HAKERÓW?

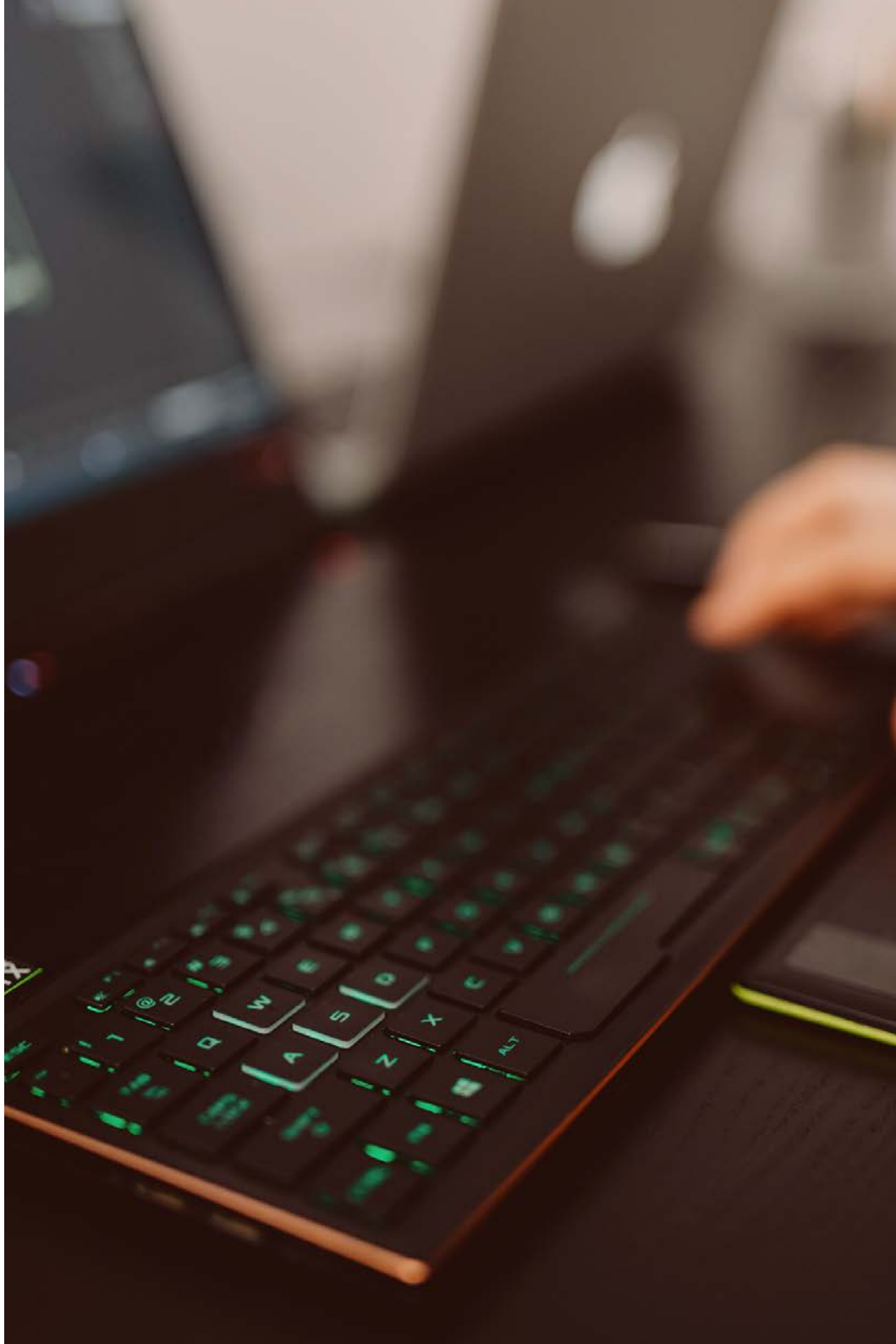
Michał Rosiak
CERT Orange Polska



W jakie pułapki wpadają pracownicy firm, jeśli chodzi o ataki hakerskie? Dlaczego w nie wpadają? Co może okazać się skuteczniejsze od antywirusa? Czy socjotechniki mogą być wykorzystywane w testach penetracyjnych? O tym rozmawiamy z Michałem Rosiakiem z CERT Orange Polska, współautorem m.in. CyberTarczy i Bezpiecznego Startera.

Jaki rodzaj socjotechniki, na podstawie Pana wiedzy i obserwacji, przestępcy wykorzystują najczęściej względem firm? Czy na przestrzeni ostatnich trzech lat sposoby ataków znacząco zmieniły się? Jak?

W tle tego wszystkiego jest ciągle wywoływanie emocji, powodowanie, aby ofiara przestała myśleć, a zaczęła reagować. Jeśli natomiast miałbym powiedzieć o zmianie podczas pandemii i wojny to porównałbym to do budowy... szczepionek mRNA. W ich przypadku „nośnik” jest niezmienny, modyfikacji podlega kod wirusa, czyli „ładunek”. W przypadku phishingu, socjotechniki, nośnikiem są wspomniane wcześniej emocje, a ładunek zależny jest od tego, co dzieje się na świecie. Stąd phishing „opakowany” w informacje o rzekomych seriach zgonów po szczepionkach, podszywający się pod „raport WHO”, czy też „atak nuklearny na Kijów”. Tak, takie też były... To jednak raczej specyfika phishingów na kradzież poświadczeń logowania do serwisów społecznościowych. Tymczasem generalnie niezmiennie mamy do czynienia z „niedopłatami rachunków”, „dopłatami do paczek”. Tu faktycznie pandemia zmieniła nieco profil, przez co najmniej pół roku przychodziły SMS-y o dopłacie na dezynfekcję paczki. Do tego jeszcze gangi ze wschodu i ich „płatności OLX”, czyli kontaktowanie się przez WhatsApp z informacją: „Już zapłaciłem, proszę kliknąć, żeby odebrać pieniądze” i wystawianie fałszywych bramek płatności albo wykradanie numerów kart.



To się nie zmienia i to przynosi największe zyski przestępcom.

Dlaczego tak się dzieje, że tyle mówi się o manipulacjach, o cyberprzestępstwach, o technikach stosowanych przez oszustów - na firmy i pracowników także - a one nadal są skuteczne?

Bo taką mamy psychikę. Emocje, które wywoła sprawny socjotechnik, dzieją się na poziomie podświadomości. „Szybko", „natychmiast", „niedopłata", „kara", „konsekwencje" – to hasła, które powodują, że serce nam szybciej bije, nawet jeśli wiemy, że to absurd, bo z jakiej racji mamy niedopłatę za prąd w firmie A, skoro od zawsze płacimy firmie B? Albo sytuacja, gdy dostajemy maila, że za 3 dni wyjeżdżamy na dwutygodniowy urlop, podczas, gdy wcale go nie planowaliśmy, bo to jeszcze nie wakacje? No to go szybko odwołam, muszę tylko kliknąć, zalogować się... No właśnie... A spojrzałaś/eś, logując się na adres w pasku przeglądarki?

Dlatego głównym hasłem edukacji świadomościowej cyberbezpieczeństwa powinno być: „Zwolnij", albo „Pomyśl". Na szkoleniach, które prowadzę, mówię: „Wiem, że masz mało czasu, a terminy siedzą i dyszą Ci w kark. Ale ile dostajesz dziennie maili, czy SMS-ów, które budzą Twoje wątpliwości? Pięć? Poświęć każdemu minutę. To jest tylko PIĘĆ MINUT. A jeśli zrobisz błąd, będzie Cię to kosztowało znacznie więcej".

„Zwolnij” i „Pomyśl”, czyli jak bronić się przed socjotechnikami hakerów?

Z drugiej strony, czego oczekiwać od dorosłych, jeżeli nawet w szkołach podstawa programowa nie przewiduje nauki związanej z cyberbezpieczeństwem... Po prostu nie jesteśmy przygotowani w tym temacie, np. podejmując pracę, gdzie ataki mogą być codziennością. Nie wiemy, nie tylko jak się bronić, ale jak możemy zostać zaatakowani.

I tu rola ludzi takich jak Adam Haertle, Piotrek Konieczny, Michał Sajdak, czy ja. Każdego, kto rozumie, o co chodzi w zagrożeniach w sieci i ma jakiekolwiek zasięgi. Jak kiedyś powiedział pierwszy z nich – i ja się z nim absolutnie zgadzam – jeśli ktoś kliknął choćby w najbardziej prostacki phishing, to wcale nie jest idiotą! To nie jego wina! Tylko nasza, bo nie dotarliśmy do niego z naszą wiedzą.

Niestety, nie mam nadziei, że zmieni się program nauczania informatyki. Zdecydowanie najlepiej by było, gdyby to młodzi uczyli nas – w końcu to oni są „digital natives”. Póki co, pozostaje jednak edukacja i mniej lub bardziej skuteczne rozwiązania techniczne. Kiedyś nazywane zbiorczo „antywirusem”, ale to też się zmienia. Dziś lepiej od antywirusa działa zdrowy rozsądek, a większym ryzykiem niż złośliwy kod, są strony przekonujące nas do podania loginów i haseł do wrażliwych serwisów.

I tu kolejne pytanie, jak są zbierane dane na temat osób, będących celem ataku w ramach socjotechniki? Czy zdobycie informacji o ofierze to skomplikowany proces?

To jest akurat proste – celem ataku może być każdy. Żeby wykraść tajne dane firmy, nie trzeba phishować prezesa! Gdy w 2013 w efekcie ataku na amerykańską sieć marketów o nazwie – nomen omen – Target wyciekły dane 43 milionów klientów, zaczęło się od przejęcia konta pracownika firmy serwisującej klimatyzację w jednym ze

stanów! Jemu wykradziono dane logowania do VPN-a Targetu, a potem, krok po kroku, przestępcy dostali się na serwery rozsyłający uaktualnienia oprogramowania do kas, gdzie wrzucili swoją wersję softu, z „niespodzianką”.

Ofiarami phishingów „wolumenowych” padają miliony losowych ludzi. Jeśli jednak chcemy trafić w konkretną osobę, czy raczej pracownika konkretnej firmy, zaryzykowałbym stwierdzenie, że skuteczność dobrego socjotechnika będzie bliska 100 procent. Same informacje w mediach społecznościowych, pozwolą atakującemu najpierw znaleźć x pracowników firmy Y, a w kolejnych krokach trafić na takiego, który udostępnia o sobie zbyt dużo. Jeśli napastnikowi bardzo zależy, może zebrać dane niczym w szpiegowskich filmach, bywając w miejscach, gdzie np. pracownicy firmy Y spotykają się na lunch (i posłuchać, co mówią, o kim i o czym), znaleźć gdzieś wzór identyfikatora firmowego, skopiować, po czym wejść komuś „na plecach” na teren firmy, by zebrać więcej informacji...
Powiedziałbym wręcz, że jeśli ktoś bardzo chce dostać się do sieci właśnie firmy Y, to szansa, że się dostanie jest bliska 100%. Pytanie brzmi, ile jest takich „firm Y”?

A czy istnieje możliwość wykorzystania socjotechnik w testach penetracyjnych? Jeśli tak, to w jaki sposób?

Jasne, że tak! Według badań poświęcenie roku na regularne kontrolowane ataki phishingowe powoduje spadek „klikających” w firmie z 31,4 do 4,8%! Ryzyko wciąż pozostaje i nigdy nie zniknie..., jest jednak nieporównywalnie mniejsze.

Dlatego warto robić to regularnie, jeśli dysponujemy odpowiednim zespołem/fachowcami – wewnętrznie – a jeśli nie, zamawiając tego rodzaju usługę, oczywiście, w przemyślany sposób, a nie z podejściem „niech ktoś nam zrobi te fiszingi”. Nie bez przyczyny US Navy Seals mawiają „Im więcej potu na ćwiczeniach, tym mniej krwi w boju”. Warto tylko pamiętać, by jedyną „karą” dla ofiar takiego phishingu było, np, przejście obligatoryjnego szkolenia. W Orange Polska absolutnie unikamy krytykowania za „wpadkę” przy kontrolowanym phishingu, stawiając na przekaz: „Wpadłeś/aś w pułapkę, ale na szczęście w naszą. Następnym razem zwróć uwagę na:” – i tu szczegółowo wypisane, na które elementy maila ofiara powinna była zwrócić uwagę. Po przeprowadzonej akcji menedżerowie dostają informację ile osób w ich jednostce dało się złapać – same liczby, bez nazwisk.

Dowodem na to, jak dobre phishingi robią moi koledzy, jest fakt, że na pierwsze dwa złapałem się sam...

Czyli rozsądek, uważność, zatrzymanie się na minutę np. przy podejrzanym mailu czy poście w social mediach i głęboki wdech wydają się przynajmniej częściowym sposobem na uniknięcie włamania do zasobów firmy. Dziękuję za rozmowę.

Rozmawiała: Monika Świetlińska

23

KONFERENCJA BRANŻY OCHRONY

POLSKA IZBA OCHRONY
rok założenia 1994

„Rola samorządu w zapewnieniu bezpieczeństwa lokalnego”

www.konferencjapio.pl

Hotel Windsor w Jachrance

06 - 07.10.2022 r.

TO PREZENTACJE PRODUKTOWE, SPOTKANIA, WYKŁADY, PANELE EKSPERCKIE O TEMATYCE:

- Technologii dla miejskiego bezpieczeństwa — dostępności usług ochronnych (monitorowanie obiektów, ochrona fizyczna, systemy bezpieczeństwa);
- Współpracy z mieszkańcami i partycypacji społecznej w tworzeniu bezpiecznych przestrzeni;
- Bezpieczeństwie lokalnych społeczności — partnerstwo sektorów prywatnego i publicznego;
- Jak organizować cyberbezpieczeństwo w lokalnym wymiarze?
- Potencjału branży ochrony dla bezpieczeństwa samorządów. Perspektywy dla Branży Ochrony oraz Ośrodków Samorządowych.

patroni medialni

a&S POLSKA

OCHRONA i BEZPIECZEŃSTWO

SECURITY MAGAZINE

partnerzy honorowi

UNIA METROPOLII POLSKICH
IM. PAWŁA ADAMOWICZA

POLSKIE REGIONY

LocalTrends
Europejskie Forum Samorządowe

securex POLAND
Międzynarodowe Targi Zabezpieczeń

partnerzy merytoryczni

RBS

SPSB

SAFETY PROJECT

PATRONAT
SECURITY MAGAZINE

KONFERENCJA BRANŻY OCHRONY

23. Konferencja Branży Ochrony odbędzie się 6 i 7 października w Hotelu Windsor, w Jachrance koło Warszawy. Po raz kolejny kilkuset uczestników reprezentujących branże ochrony, ekspertów z dziedziny security, instytucji bezpieczeństwa, przedsiębiorców z sektora ochrony i zabezpieczeń, a także reprezentanci samo-rządów lokalnych spotkają się w Jachrance, by omówić: „Rolę samorządu w zapewnieniu bezpieczeństwa lokalnego".

Podczas tego spotkania odbędą się prezentacje, panele eksperckie, prezentacje produktowe oraz networking. Dzięki współpracy z Partnerami Polskiej Izby Ochrony będą Państwo mogli poszerzyć swoją wiedzę dotyczącą najnowszych rozwiązań bezpieczeństwa samorządów lokalnych.
Polska Izba Ochrony (PIO) jako wiodąca organizacja przedsiębiorców w sektorze bezpieczeństwa, zrzesza około 180 firm współpracujących z podmiotami prywatnymi i publicznymi, w tym samorządem terytorialnym, w realizacji zadań ochronnych w Rzeczypospolitej Polskiej. Mamy przekonanie, że lokalny poziom bezpieczeństwa – gmina, miasto, powiat i metropolie to kluczowe obszary aktywności administracji, przede wszystkim samorządowej oraz Policji, służb i straży podejmujących codzienny wysiłek zmierzający do ograniczania zagrożeń dla mieszkańców, zapobiegania kryzysom i właściwego reagowania w przypadku identyfikacji niebezpieczeństw.

Konferencja jest adresowana do władz miast, gmin, powiatów i urzędów marszałkowskich oraz przedstawicieli komórek/jednostek odpowiedzialnych za bezpieczeństwo i zarządzanie kryzysowe w tych podmiotach.

Podczas tego spotkania chcemy pokazać potencjał branży ochrony i zaprezentować jej wpływ dla miejskiego bezpieczeństwa.

Konferencję wystąpieniami uświetnią:

- Pan Jacek Jaśkowiak, prezydent Miasta Poznania,
- Pan Generał Waldemar Skrzypczak, generał broni, dowódca Wojsk Lądowych RP w latach 2006-2009,
- Pan Andrzej Nowakowski, prezydent Miasta Płocka.

Jak zarejestrować się na 23. Konferencję Branży Ochrony?

1. Wypełniając formularz on-line:
Formularz rejestracyjny - **wersja polska**
Formularz rejestracyjny - **wersja angielska**
2.Odsyłając wypełnione i zeskanowany formularz zgłoszeniowy na adres e-mail:
biuropio@piooim.pl

Kontakt: pon - pt w godz. 8 - 16
tel. (22) 635-28-29, tel. kom: 696 719 615
mail: biuropio@piooim.pl

SECURITYMAGAZINE.PL

BEZPIECZEŃSTWO W SIECI, CYBERWOJNA, FAKE NEWSY. 22. KONGRES PR

PATRONAT
SECURITY MAGAZINE

Podczas konferencji, która odbyła się 15- 16 września, poruszone zostały zagadnienia dezinformacji i cyberbezpieczeństwa. Eksperci dyskutowali też o narzędziach wspomagających reagowanie w sytuacji kryzysu wizerunkowego oraz o cyberatakach, które dla firm stanowią poważne zagrożenie w dobie cyfryzacji.

W trakcie dwóch dni pełnych edukacji i inspiracji, specjaliści od komunikacji wygłosili kilkanaście prelekcji, dzięki którym 200 uczestników z całej Polski stało się bogatszymi o wiedzę w zakresie radzenia sobie z dezinformacją i cyberatakami w kontekście komunikacji wewnętrznej oraz zewnętrznej. Branża PR rozmawiała o sposobach walki z problemem, który zdominował media, zwłaszcza od czasu rozpoczęcia wojny w Ukrainie.

CYFRYZACJA, TECHNOLOGIE, KOMUNIKACJA IT Z PR, DEZINFORMACJA

O tym, jak ważna jest synergia między IT i PR mówili podczas debaty **Beata Łaszyn, wiceprezeska Alert Media Communications, Krzysztof Moczulski, rzecznik prasowy PLL LOT, Marta Andreasik, PR Manager, Huuuge Games, Sebastian Bykowski, prezes zarządu, dyrektor generalny PRESS-SERVICE Monitoring & More, Michał Rosiak, ekspert i edukator cyberbezpieczeństwa z CERT Orange, Błażej Szymczak, chief security officer z Modivo oraz Bartosz Sowier, dyrektor departamentu analiz i legislacji z Pracodawcy PR.**

Michał Rosiak podkreślił, jak na przestrzeni dekady zmieniło się podejście wewnątrz przedsiębiorstwa do osób zajmujących się cyberbezpieczeństwem. - *W firmie nie powinno być podziału na Wy-My. Trzeba w organizacji mówić tym samym językiem. Dostosowywać się do rozmówców. Dotyczy to również "bezpieczników"* - zaznaczył.

Bezpieczeństwo w sieci, cyberwojna, fake newsy.
22. Kongres PR

Współpraca wewnątrz firmy jest kluczem do efektywnych działań na rzecz jej ochrony i wspierania, kiedy zdarzy się incydent. - *To porozumienie powinno nastąpić tak szybko, jak się da. Dla wspólnego dobra. Bo my, pijarowcy i bezpiecznicy, od siebie zależymy. Ta synergia jest czymś kluczowym i albo to zrozumiemy i wejdziemy razem w tę współpracę, albo coś nie będzie działało w naszej organizacji* - podkreśliła **Marta Andreasik.**

- PR musi rozumieć pojęcia, znać podstawowe zagadnienia związane z cyberbezpieczeństwem. Z kolei pracownicy z działów bezpieczeństwa potrzebują umiejętności komunikacyjnych, żeby dobrze wszystko przekazać. Dlatego potrzebne są rozmowy - zaznaczyła **Beata Łaszyn**, dodając, że każdy dział w firmie musi ze sobą współpracować i wzajemnie się rozumieć: - *Standardowo to wygląda tak, że kiedy jest np. wyciek danych, do bezpiecznika przychodzi PR-owiec i pyta o szczegóły. I prawdopodobnie nie otrzyma żadnej informacji, bo są sytuacje, kiedy po pierwsze, nie wiadomo tego od razu, po drugie, żeby to było wiadomo, potrzeba czasu. A PR-owiec przecież musi coś przekazać mediom, bo informacja o wycieku dotarła już do opinii publicznej. PR-owiec musi być też gotowy na to, że tej odpowiedzi od bezpieczeństwa nie dostanie szybko. Musi to rozumieć i wiedzieć, jakie są zagrożenia.*

O tym jak istotna jest komunikacja między działami IT a PR wspomniał **Sebastian Bykowski z PRESS-SERVICE**, zauważając, że wszystkie zagrożenia związane z bezpieczeństwem, potrafią naruszać reputację firmy. - *Firmy zamawiają monitoring tego, co i jak mówi się w sieci na temat związany z bezpieczeństwem, zachowaniem bezpieczeństwa danych o klientach, tego czy one mogą czuć się bezpiecznie. W zależności od branży, widzimy, że odsetek infor-*

Bezpieczeństwo w sieci, cyberwojna, fake newsy.
22. Kongres PR

SECURITYMAGAZINE.PL

macji korporacyjnych, w ponad 30% potraf dotyczyć w danej firmie samego bezpieczeństwa i bezpieczeństwa IT. I to jest ogromny skok, bo jeszcze przed pandemią to było dosłownie kilka procent. Te tematy, krążące w internecie, mogą obniżyć reputację marki, a jest to niepożądane w sytuacji, kiedy w szczególności firma chce budować wizerunek marki, która jest blisko konsumenta, która dobrze dopasowuje produkt do jego oczekiwań - przekazał Bykowski.

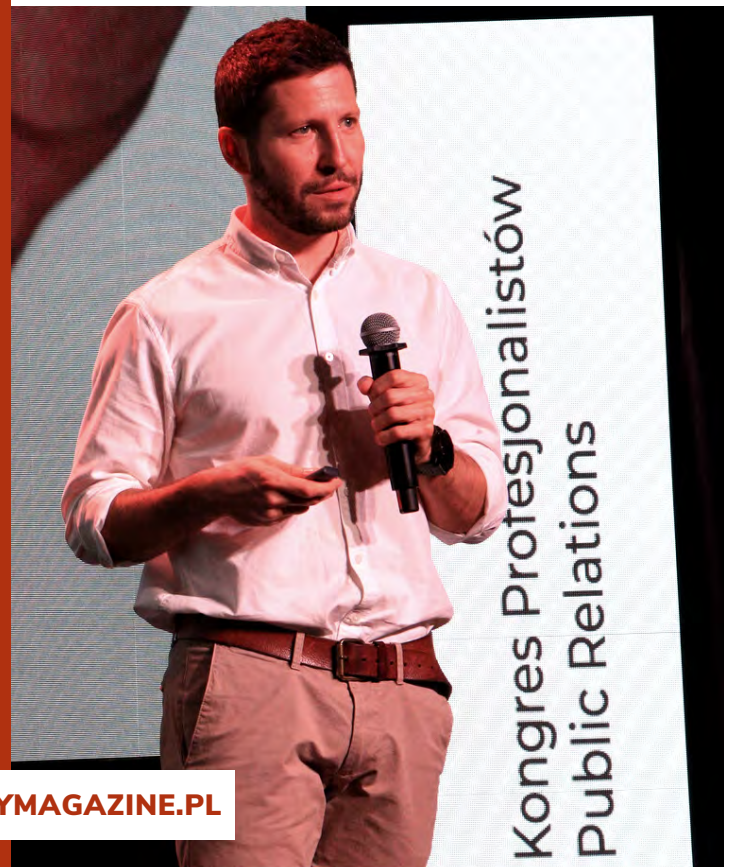
O dezinformacji rozmawiali podczas drugiej debaty **Tomasz Kułakowski, rzecznik prasowy Krynica Vitamin, były wieloletni korespondent Polsatu w Moskwie, Karolina Łuczak, rzeczniczka prasowa Provident Polska, Małgorzata Bajer, dyrektor ds. komunikacji, promocji i marketingu, rzecznik prasowy PGE Narodowy, Katarzyna Kopeć-Ziemczyk, kierowniczka komunikacji Polada, Anna Kulbicka-Tondel, rzeczniczka prasowa Miasta Torunia, Arkadiusz Szczepański, dyrektor generalny Jacobs&Schwartz.**

Na scenie tego dnia mówili również, zwłaszcza o wyzwaniach w komunikowaniu, **Adam Łaszyn z Alert Media Communications, Anna Klimczuk z Microsoft, Łukasz Borowicz z OLX Praca, Monika Borzdyńska z PGE Narodowy, Aida Bella z Totalizatora Sportowego, MAksymilian Pawłowski z Teknos i Tomasz Popielawski z Ceramika Paradyż.**

O CYBERBEZPIECZEŃSTWIE

Drugi dzień Kongresu zdominował temat cyberbezpieczeństwa. Dyskusja o zagrożeniach związanych z funkcjonowaniem w sieci została podjęta m.in. w debacie „Cyberbezpieczeństwo jako wyzwanie dla procesów komunikacyjnych XXI wieku”, prowadzonej przez Nell Przybylską, dyrektor ds. PR i Komunikacji

Bezpieczeństwo w sieci, cyberwojna, fake newsy.
22. Kongres PR



w Fundacji Digital Poland. Jej gośćmi byli: **Alicja Skraburska, cybersecurity technical lead z HSBC, Piotr Ślusarczyk, product manager z netPR.pl, płk dr Piotr Potejko, specjalista w obszarze bezpieczeństwa, ekspert Instytutu Staszica, preze zarządu w ASIS Polska, płk rez. dr Dariusz Kryszk z Zakładu Komunikacji Strategicznej z Akademii Sztuki Wojennej oraz Łukasz Świerżewski, członek zarządu Polskiej Agencji Prasowej.** Ostatni z gości zaprezentował również wyniki ankiety związanej z cyberbezpieczeństwem, o której pisaliśmy w sierpniowym wydaniu "Security Magazine".

Na pytanie, jak uniknąć pułapek i kryzysu wizerunkowego w czasie cyberataku odpowiadali **Magdalena Grochala, ekspertka w zakresie komunikacji i public relations z agencji Symetria PR i Mariusz Prociewicz, CISO w Silky Coders z Grupy Kapitałowej LPP.** O cyberbezpieczeństwie jako elemencie budowy tożsamości korporacyjnej mówiła Anna Olszewska, dyrektor departamentu komunikacji w Krajowej Izbie Rozliczeniowej S.A. Deniz Rymkiewicz, rzecznik prasowy Grupy eSky zdradził sposoby na wyprzedzanie kryzysów oraz zabezpieczanie firmy przed kryzysami.

Bezpieczeństwo w sieci, cyberwojna, fake newsy.
22. Kongres PR

O fake newsach opowiedział też gość specjalny Kongresu – **podpułkownik Brett Lea – oficer ds. public affairs w 82. Dywizji Powietrznodesantowej armii amerykańskiej.** Wykładowca historii wojskowości w Akademii Wojskowej Stanów Zjednoczonych w West Point w rozmowie z **Bartoszem Staniszewskim, CEO Brandfeed**, wyjaśnił, jak wygląda sposób komunikacji z mediami i społecznością lokalną w trakcie wojny. Na scenie drugiego dnia pojawili się również: **Monika Tenerowicz, kierowniczka wydziału relacji z mediami z Orange Polska i prof UJ, dr hab. Jarosław Flis, płk rez. dr Dariusz Kryszk z Zakładu Komunikacji Strategicznej z Akademii Sztuki Wojennej.**

Kongres Profesjonalistów Public Relations w Rzeszowie, którego organizatorem jest firma **Newsline Sp. z o.o.**, od 22 lat łączy środowisko i ludzi zajmujących się problematyką komunikacji i PR. Stanowi forum dialogu, inspiracji i integracji wszystkich tych, którzy tworzą branżę: praktyków, naukowców i pasjonatów.

Fot. Monika Świetlińska, mat. prasowe organizatora

Bezpieczeństwo w sieci, cyberwojna, fake newsy.
22. Kongres PR

ZOSTAŃ EKSPERTEM

SECURITY MAGAZINE

PROMUJ SWOJĄ MARKĘ! BUDUJ WIZERUNEK SWOJEJ FIRMY LUB SIEBIE SAMEGO, SIEBIE SAMEJ

REDAKCJA@SECURITYMAGAZINE.PL

KOMUNIKACJA W CZASIE CYBERATAKU

Magdalena Grochala
Symetria Public Relations

Mariusz Prociewicz
Silky Coders

Cyberatak to dla firmy sytuacja kryzysowa – problem technologiczny, finansowy i wizerunkowy, bo utrata danych – czy to klientów, czy pracowników lub partnerów biznesowych – oznacza także utratę ich zaufania. Zatem czy w ogóle informować opinię publiczną o ataku cyberprzestępców? I jak to robić?

Zacznijmy od tego, że cyberatak może zdarzyć się każdej firmie – nawet tej najlepiej przygotowanej i posiadającej najnowocześniejsze zabezpieczenia. Tylko we wrześniu 2022 roku media poinformowały o cyberatakach na Ubera i Revoluta. W 2021 roku łupem cyberprzestępców padły takie marki jak LinkedIn, Android, Panasonic, T-Mobile czy Microsoft. W poprzednich latach ze skutkami działań hakerów mierzyły się Twitter czy Yahoo. W sumie co roku wyciekają dane setek milionów użytkowników.

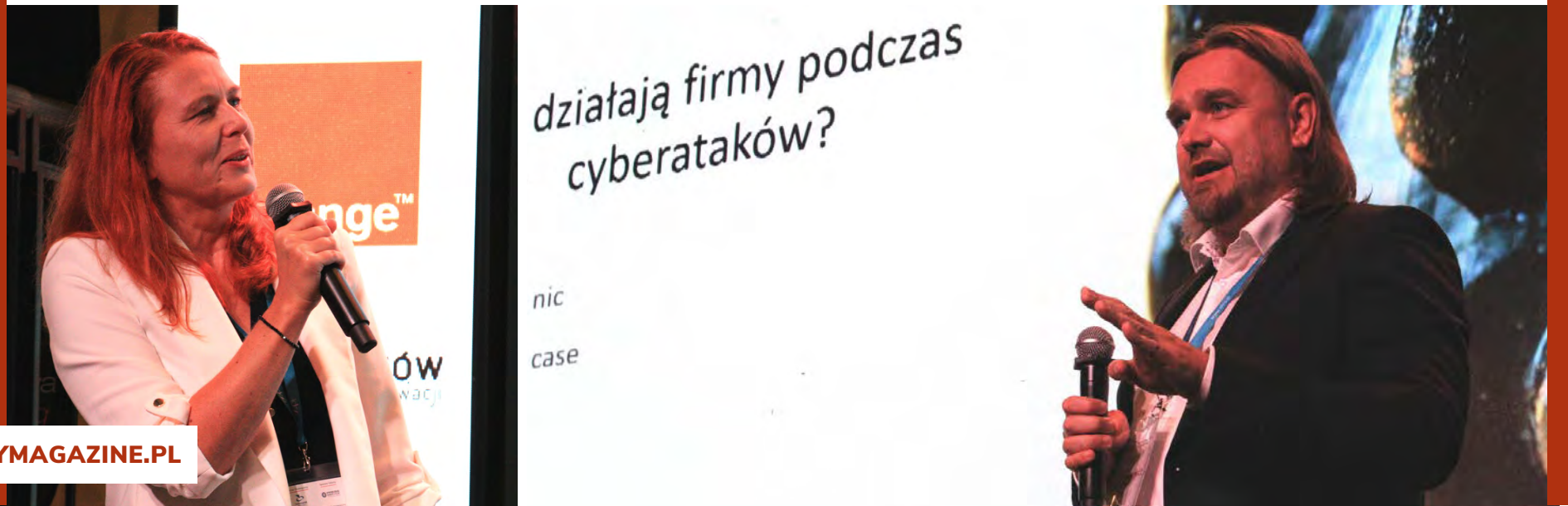
Statystyki nie pozostawiają złudzeń – według Accenture liczba ataków wzrosła od 2014 roku o 67%.

Badania Varonis pokazują, że jedynie 5% firm jest odpowiednio chronionych. Z danych Sophos wynika, że aż 54% przedsiębiorstw twierdzi, iż nie poradzi sobie z zaawansowanymi cyberatakami.

IBM wyliczył, że średni koszt naruszenia danych w 2021 roku wyniósł 4,24 miliona dolarów.

Wniosek? Jest źle, a będzie jeszcze gorzej albo przynajmniej tak samo. Pytanie nie brzmi więc, „czy", a „kiedy" firma czy organizacja zostanie zaatakowana bądź zmierzy się z poważnym incydentem bezpieczeństwa, którym może być, na przykład, wyciek danych spowodowany ludzkim błędem.

MAGDALENA GROCHALA I MARIUSZ PROCIEWICZ PODCZAS KONGRESU PR.



FINANSOWE I WIZERUNKOWE SKUTKI CYBERATAKU

Incydenty bezpieczeństwa – zwłaszcza te, w wyniku których wyciekają dane klientów, pracowników czy kontrahentów firmy – przekładają się na spadek zaufania do niej. To jeden z najpoważniejszych skutków cyberataku. Ale niejedyny. Jeśli organizacja jest źle przygotowana do takiej sytuacji kryzysowej i reaguje nieodpowiednio, rezultatem są także zmiany personalne, często na wysokich stanowiskach.

To kolejny krok do wzbudzenia niepokoju wśród klientów czy inwestorów. Narastający brak zaufania odbija się na cenach akcji. W 2021 roku na portalu Comparitech została opublikowana ciekawa analiza obejmująca 34 spółki notowane na nowojorskiej giełdzie papierów wartościowych i 40 dużych incydentów bezpieczeństwa, które wydarzyły się w tych firmach. Dane jasno pokazały, że ujawnione naruszenia bezpieczeństwa miały bezpośredni, niekorzystny wpływ na cenę akcji i był on odczuwalny nawet długo po ataku, chociaż, oczywiście, z biegiem czasu malał.

W wyniku działań cyberprzestępców cierpi więc budżet firmy, i tak przeciążony koniecznością walki z technologicznymi skutkami ataku. Do tego mogą dojść kary za niepoinformowanie o zdarzeniu lub za nieodpowiednią ochronę danych osobowych. A to wszystko – zwłaszcza w atmosferze złej komunikacji, niedomówień, czasem nawet kłamstw i mijania się z prawdą, a także przy wzmożonym zainteresowaniu klientów i mediów oznacza tylko jedno – **kryzys wizerunkowy.**

W łagodzeniu jego skutków pomaga odpowiednia komunikacja. To, w jaki sposób firma zareaguje na wiadomość o ataku lub incydencie i w jaki sposób poinformuje o tym opinię publiczną, jest kluczowe i może pomóc w minimalizowaniu negatywnego wpływu ataku na poziom zaufania do przedsiębiorstwa.

MÓWIĆ CZY NIE MÓWIĆ? CO NA TO PRAWO?

Gdy dochodzi do cyberataku, firmy często zastanawiają się, czy powinny o tym poinformować media oraz klientów. A może lepiej zachować atak w tajemnicy? Wskazówki w tym zakresie daje polskie prawo, w którym są zapisy mówiące o obowiązku informowania odpowiednich organów o incydentach bezpieczeństwa.

Przykładem jest Rozporządzenie o Ochronie Danych Osobowych (RODO), które nakłada na administratora danych obowiązek zgłoszenia naruszenia ochrony danych organowi nie później niż w terminie 72 godzin po stwierdzeniu takiego naruszenia (art. 33). Dodatkowo administrator ma również obowiązek zawiadomienia o naruszeniu osoby, której dane dotyczą, w przypadku, gdy istnieje ryzyko naruszenia praw i wolności tej osoby (art. 34).

Ustawa o krajowym systemie cyberbezpieczeństwa (dyrektywa NIS) nakazuje operatorom usług kluczowych (energetyka, banki, finanse, transport, ochrona zdrowia itd.) zgłoszenie incydentu bezpieczeństwa do 24h od momentu wykrycia. Dostawcy usług płatniczych są natomiast w świetle dyrektywy PSD2 zobowiązani do niezwłocznego zgłoszenia incydentu.

To oznacza tylko jedno – w niektórych przypadkach firma nie może samodzielnie decydować, czy informować o incydencie, czy nie. Musi za to zawiadomić odpowiednie organy oraz poszkodowane osoby. A co jeśli tego nie zrobi? Zaniechanie tego obowiązku może się okazać bardzo kosztowne.

W Polsce przekonało się o tym choćby Towarzystwo Ubezpieczeń Warta, które zapłaciło 85 588 zł kary za świadomie nieinformowanie Urzędu Ochrony Danych Osobowych o incydencie naruszenia danych klienta oraz za niepoinformowanie rzeczonego klienta o wycieku jego danych.

PRZYGOTOWAĆ SIĘ DO CYBERATAKU

Dobra wiadomość jest taka, że do cyberataku – jak do każdej sytuacji kryzysowej – można się przygotować. Przede wszystkim warto pamiętać o tym, że w czasie takiego kryzysu znaczącą rolę odgrywa komunikacja, czyli dział PR. I to ten dział, czy osoby odpowiedzialne za komunikację wewnętrzną i zewnętrzną, muszą być wraz z działem bezpieczeństwa współodpowiedzialne za przygotowanie strategii działania w czasie cyberataku.

To PR pomaga w budowaniu świadomości – począwszy od ustalenia wytycznych, reguł, na podstawie których można stwierdzić, kiedy zaczyna się kryzys wizerunkowy, a kiedy to tylko incydent rangi **'business as usual'**. To PR pomaga także w przygotowaniu komunikatów dla pracowników, przekazujących wytyczne działów bezpieczeństwa i IT, wyjaśniających, jak działają hakerzy i na co zwracać uwagę w codziennej pracy, by unikać pułapek zastawianych przez cyberprzestępców.

PR monitoruje także otoczenie, prasę, informacje w Internecie i ma wiedzę oraz doświadczenie, którymi sygnałami należy się zająć.
A nade wszystko koordynuje działania komunikacyjne wewnątrz i na zewnątrz organizacji.

Wraz z działami bezpieczeństwa, IT, HR-em oraz działem prawnym może też przygotować firmę na cyberatak. Strategia działania na wypadek wystąpienia takiego kryzysu musi zawierać między innymi skład sztabu kryzysowego z aktualnymi danymi teleadresowymi do wszystkich osób znajdujących się w tym sztabie (także danych alternatywnych, z których można skorzystać, gdy nie działa służbowa poczta oraz telefony), wyznaczone role i odpowiedzialności, kategorie incydentów, plan eskalacji w przypadku wystąpienia tych incydentów, gotowe wzorce odpowiedzi dopasowane do kategorii incydentu i do grup interesariuszy. Dzięki temu firma będzie w stanie szybko zidentyfikować potencjalny problem oraz natychmiast wdrożyć odpowiednią strategię komunikacji, która pozwoli jej zareagować na incydent, zanim zrobią to jej klienci oraz media.

SKUTECZNA KOMUNIKACJA W 7 KROKACH

W przypadku cyberataku niezwykle ważna jest komunikacja z wieloma grupami interesariuszy – z pracownikami, inwestorami, klientami, partnerami biznesowymi.

I w końcu z mediami.

Jak robić to skutecznie?

ŚCISŁA WSPÓŁPRACA NA LINII PR – DZIAŁ IT

W czasie cyberataku podstawą jest bardzo dobra współpraca i ciągły kontakt działu PR z działami bezpieczeństwa i IT odpowiedzialnymi za analizę i usuwanie skutków ataku. Cyberbezpieczeństwo jest trudnym tematem, a naruszenie bezpieczeństwa poważną sytuacją, stąd PR i IT muszą współdziałać, by przekazać zainteresowanym rzetelne i zrozumiałe informacje.

PEWNOŚĆ I DOWODY

Komunikacja nie może wyprzedzać faktów. Jeśli firma nie ma pewności, czy problem z działaniem infrastruktury rzeczywiście wynika z cyberataku, i nie wie, czy jakiekolwiek dane ucierpiały – nie powinna sugerować tego w komunikatach przekazywanych opinii publicznej (usprawiedliwiając na przykład dużą awarię domniemaniami o możliwym ataku hakerskim).

OSTROŻNOŚĆ W PODEJMOWANIU DZIAŁAŃ

Mówiąc o cyberataku, firma musi być bardzo ostrożna. Atak wiąże się także z koniecznością zgłoszenia do UODO, zatem to, co firma przekazuje w dokumentach do urzędu, i komunikaty w mediach czy social mediach muszą być spójne.

DOBRE WYCZUCIE CZASU

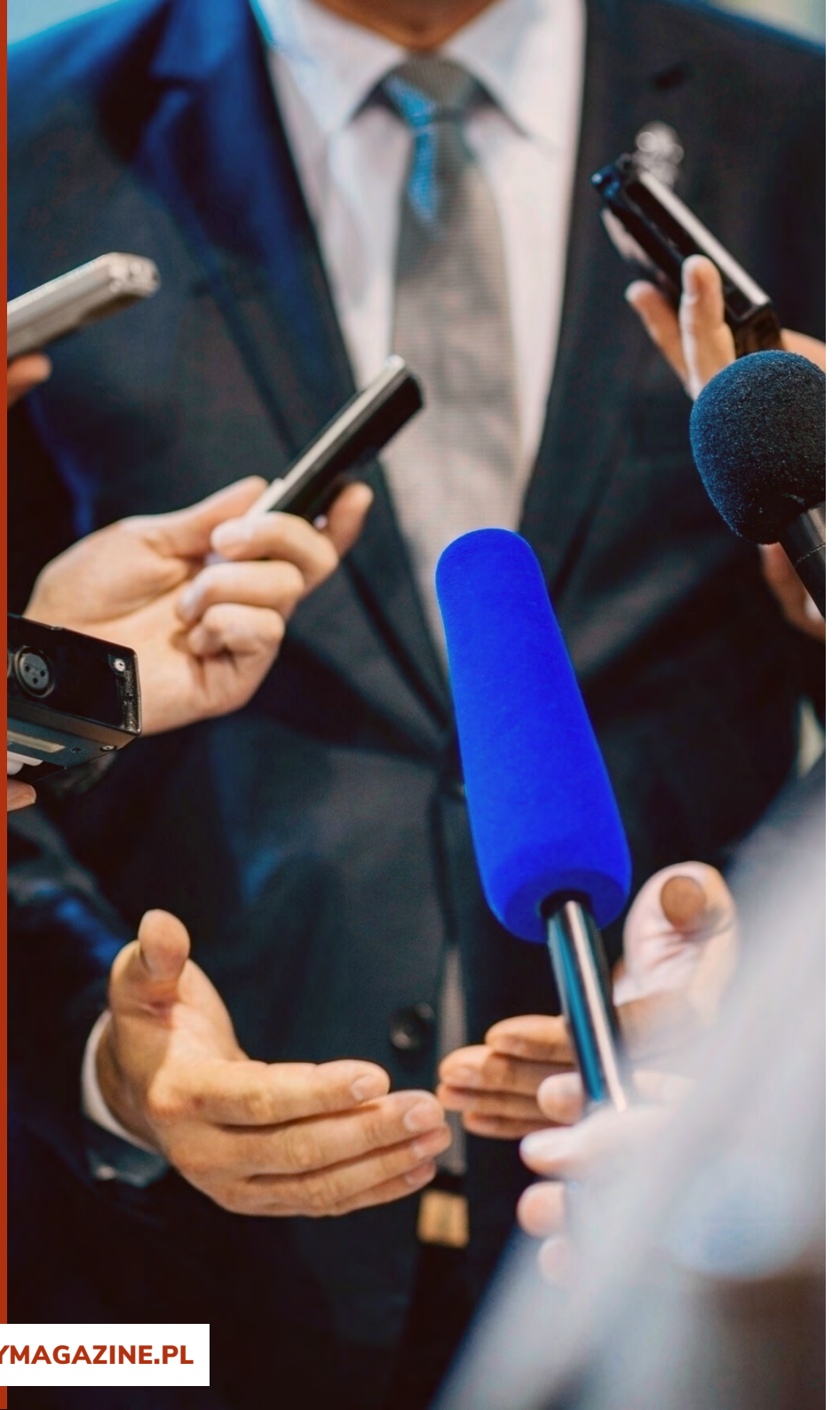
Komunikację należy zacząć, gdy firma ma pewność, że nastąpił cyberatak. A kiedy ją skończyć? Najlepiej w momencie, gdy problem jest już opanowany. Nie ma potrzeby przypominania o ataku długo po nim, choć oczywiście jeśli przedsiębiorstwo podejmie ważne działania poprawiające jego bezpieczeństwo, może o tym także poinformować klientów i kontrahentów.

WYPRZEDZANIE REAKCJI KLIENTÓW/UŻYTKOWNIKÓW

Najważniejsze jest jednak to, aby zacząć komunikację, zanim zrobią to klienci czy użytkownicy usługi. A zaczną ją z całą pewnością, bo informacja o tym, że ich dane wyciekły lub że usługa nie działa, w końcu do nich trafi. W dobie social mediów taka wiadomość rozejdzie się aż za szybko. Jeśli to zaatakowana firma zainicjuje komunikację, łatwiej będzie jej nadać ton całemu przekazowi.

INFORMOWANIE I WYJAŚNIANIE

Wyciek danych oznacza niepokój po stronie klientów czy pracowników. Zadaniem firmy jest



więc nie tylko poinformowanie ich o naruszeniu, ale również wyjaśnienie, jakie kroki mają teraz podjąć.

SPÓJNOŚĆ W KOMUNIKACJI

Cyberatak to poważna sytuacja i należy z odpowiednią powagą o nim mówić. Niezależnie od kanału komunikacji. Jeśli firma korzysta z różnych mediów (www, Facebook, Instagram), jej przekazy w tych miejscach muszą mieć podobny ton i treści.

Im więcej firmy mówią o cyberatakach – rzetelnie i transparentnie – im częściej pokazują, jak funkcjonują w czasie ataku, tym lepiej do takich sytuacji mogą przygotować się także inni.

Odpowiednia komunikacja, opierająca się na planie kryzysowym i współpracy działów IT oraz PR, nie tylko pozwoli zminimalizować skutki ataku, ale też pomoże edukować rynek i w ostatecznym rozrachunku – skuteczniej walczyć z cyberprzestępcami.

Walutomat®

Wymieniaj walutę online - korzystnie i bezpiecznie 24/7

Największa platforma wymiany walut w Polsce

Korzyści:

- Szybkie i korzystne przelewy zagraniczne **do ponad 50 krajów**
- Przelew natychmiastowy w **EUR - SEPA Instant**
- Szybka wpłata kartą płatniczą, QR kodem, BLIK lub PayPal
- Intuicyjna **aplikacja mobilna**

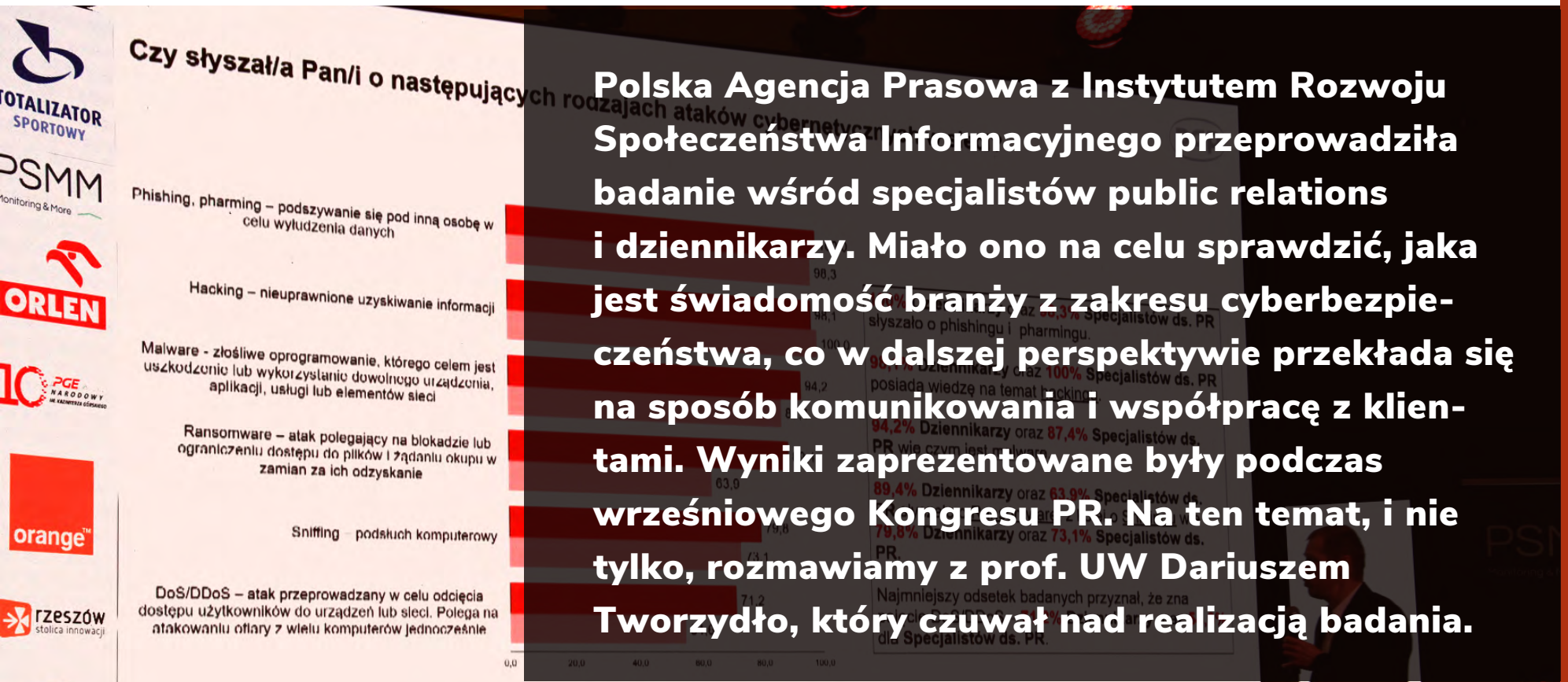
Dowiedz się więcej na **www.walutomat.pl**

Zeskanuj kod i odbierz rabat

Kupon ważny w terminie 20.09.2022 - 31.01.2023

CYBERBEZPIECZEŃSTWO W BRANŻY PR I W MEDIACH

Dariusz Tworzydło
EXACTO



Polska Agencja Prasowa z Instytutem Rozwoju Społeczeństwa Informacyjnego przeprowadziła badanie wśród specjalistów public relations i dziennikarzy. Miało ono na celu sprawdzić, jaka jest świadomość branży z zakresu cyberbezpieczeństwa, co w dalszej perspektywie przekłada się na sposób komunikowania i współpracę z klientami. Wyniki zaprezentowane były podczas wrześniowego Kongresu PR. Na ten temat, i nie tylko, rozmawiamy z prof. UW Dariuszem Tworzydło, który czuwał nad realizacją badania.

Czy wyniki ankiety przeprowadzonej wspólnie z PAP są dla Pana zaskoczeniem? Które z odpowiedzi na pytania czy problemy poruszone w ankiecie zaskoczeniem nie były?

Wyniki przeprowadzonych badań z pewnością potwierdziły przypuszczenia, że zarówno dziennikarze, jak i PR-owcy chronią swoją dane, potrafią rozpoznać maile z zagrożeniem. Są świadomi tego, że na przestrzeni ostatnich lat odnotowywany jest w sieci stały wzrost cyberprzestępstw, związanych z utratą lub przejęciem danych. Ponadto, często zauważają w mediach społecznościowych wpisy, których autorami są boty. Pewnego rodzaju zaskoczeniem może być natomiast fakt, że specjaliści ds. public relations postrzegają swoją grupę zawodową jako najmniej zagrożoną cyberatakami. Jako ciekawostkę podam również, że co drugi respondent przyznaje, że zawsze zakrywa obiektyw kamery w laptopie.

Ankieta skoncentrowana była wokół tematyki cyberbezpieczeństwa w agencjach PR, ale także w redakcjach mediów. Czy te dwa światy bardzo różnią się od siebie, jeśli chodzi o dbanie o swoje bezpieczeństwo?

Odpowiedzi udzielane przez obie grupy bardzo często były zbieżne, jednak można wyróżnić kilka miejsc, w których różnice były istotne. Dla przykładu, badani dziennikarze zdecydowanie częściej przyznawali, że zdarzyło się im utracić ważne dane. Wiąże się to zapewne z tym, że, jak sami przyznają, otrzymują oni w ciągu dnia znacznie więcej maili, które są spamem lub potencjalnym atakiem hakerskim. Ponadto, z uwagi na charakter swojej pracy, dziennikarze znacznie częściej od PR-owców korzystają z publicznych sieci Wi-Fi. Większa liczba specjalistów ds. public relations deklarowała natomiast, że firmy z ich branży są dobrze zabezpieczone przed atakami cybernetycznymi. Co ciekawe, to dziennikarze częściej wskazywali, że regularnie poszerzają swoją wiedzę na temat cyberbezpieczeństwa.

Jakie wnioski wyciągnął Pan z ankiety? Jest dobrze, źle, mogłoby być lepiej? Co możemy zrobić, by lepiej się stało, biorąc pod uwagę cyberbezpieczeństwo w branży PR i w mediach?

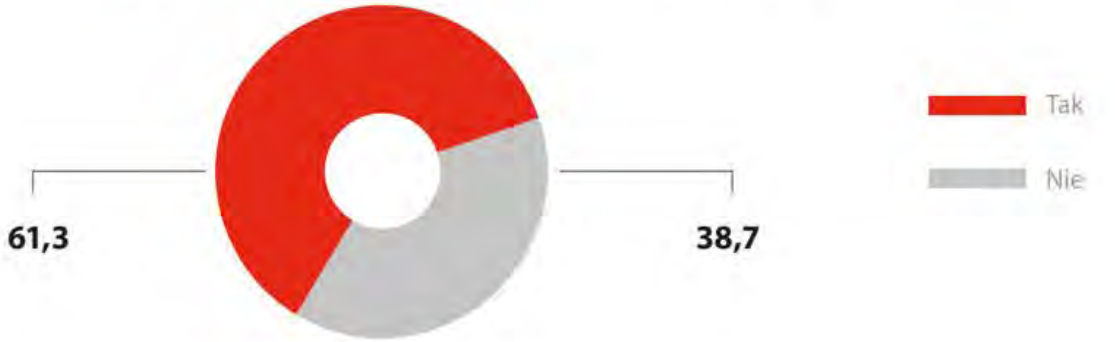
Uważam, że jest dobrze. Z badań wynika, iż dziennikarze oraz PR-owcy zabezpieczają swoje dane w Internecie oraz te, które są przechowywa-

ne na prywatnym czy służbowym sprzęcie. Również poziom wiedzy na temat rodzajów ataków cybernetycznych w sieci określiłbym jako wysoki. Widoczny jest jednak brak znajomości takich pojęć jak ransomware, sniffing, czy DoS/DDoS. Należy w dalszym ciągu poszerzać swoją wiedzę na temat cyberbezpieczeństwa i odbywać szkolenia, gdyż pomogą one skutecznie bronić się przed cyberatakami.

Wróćmy do Kongresu. Niemal całe dwa dni poświęcone były bezpiecznemu korzystaniu z nowych technologii, ale także dezinformacji czy współpracy między działami bezpieczeństwa i działami PR. Jaki priorytet dla pijarowców ma dziś cyberbezpieczeństwo? Czy w ogóle jest priorytetem?

Dla świadomych specjalistów PR cyberbezpie-

WYKRES 7. CZY PANA/I FIRMA NA BIEŻĄCO INFORMUJE PRACOWNIKÓW O ZAGROŻENIACH I INSTRUUJE ICH JAK SIĘ ZABEZPIECZAĆ? N=119 (W %)



Wartości na wykresie zostały zaokrąglone, przez co mogą nie sumować się do 100%

Źródło: opracowanie własne na podstawie badania PR-owców

JEDNO Z PRZYKŁADOWYCH PYTAŃ W ANKIECIE.

czeństwo to priorytet. Każdy zdaje sobie bowiem sprawę z tego, że cyberzagrożenia są współcześnie tak duże, że problem ten musi być brany pod uwagę jako jeden z kluczowych do rozwiązania. Dotyczy to zarówno relacji z klientami, jak i komunikacji wewnętrznej w firmach. Zawarte w raporcie wyniki badań jasno pokazują, że wiedza z zakresu cyberbezpieczeństwa jest w branży PR coraz szerzej propagowana i stale pogłębiana.

W Kongresie uczestniczyło ok. 200 PR-owców z całej Polski. Jak Pan ocenia ich zainteresowanie tematami poruszanymi w tym roku?

Temat jest aktualny i trudno pozostać wobec niego obojętnym. Zwłaszcza w perspektywie rozpowszechnianych dezinformacji i cyberzagrożeń w związku z wojną w Ukrainie i, nieco wcześniej, pandemią COVID-19. PR-owcy również mają tego świadomość, dostrzegają wagę problemu oraz to, jak silnie oddziałuje on na całą branżę. Zjawisko to mocno determinuje poziom zaufania społecznego, a co za tym idzie, wpływa na komunikację z klientami, a nawet pracownikami. Jestem pewien, że w dalszej perspektywie uwarunkuje metody komunikacji wewnętrznej i zewnętrznej.

Czy rozmowy z Kongresu dotyczące cyberbezpieczeństwa będą miały swoją kontynuację? Wielu uczestników zaznaczało, że w ciągu tych dwóch dni zrodziło się wiele cennych pomysłów, wskazano kilka istotnych aspektów np. związanych ze współpracą między bezpiecznikami a działami komunikacji. Mówiono, że tematy poruszane podczas Kongresu to fundamenty dobrych praktyk, które powinny mieć swój ciąg dalszy.

Tak jak wspomniałem, dezinformacja i cyberprzestępstwa to problem, który będzie eskalował. Z całą pewnością konieczne będzie pogłębianie wiedzy w tym zakresie. Współczesne wyzwania wymagają od branży PR dużej elastyczności, sprawnego i skutecznego reagowania na stale rozwijające się zagrożenia. Jestem przekonany, że tegoroczny Kongres to tylko początek szerokiej dyskusji na ten temat. Bardzo się cieszę, że to spotkanie stało się okazją do usystematyzowania wiedzy w zakresie cyberbezpieczeństwa, co pomaga ją rozpowszechniać, ale również ukazuje białe plamy, wymagające jeszcze uzupełnienia i dalszych analiz.

Rozmawiała: Monika Świetlińska

WYKRES 2. CZY W OSTATNIM MIESIĄCU SPOTKAŁ/A SIĘ PAN/I Z ATAKIEM MAJĄCYM NA CELU USUNIĘCIE LUB PRZEJĘCIE DANYCH, KTÓRY TO ATAK BEZPOŚREDNIO DOTYCZYŁ PANA/I? N=104 (W %)

Wartości na wykresie zostały zaokrąglone, przez co mogą nie sumować się do 100%

Źródło: opracowanie własne na podstawie badania dziennikarzy

PANCERNIK IT

TWORZYMY BEZPIECZNE IT

Pancernik Security Show

Strefa dla pasjonatów bezpieczeństwa IT

400 uczestników
50 wystawców expo
4 sale prelekcyjne
warsztaty
cyber-laboratoria

28 października 2022

Katowice,
Hotel Vienna House Easy

tylko dla czytelników
10 bezpłatnych biletów
podaj kod: IPv7

Adam Haertle

Redaktor | Zaufana Trzecia Strona

Uznany prelegent, trener i wykładowca. Potężna dawka wiedzy i rozrywka w jednym. Redaktor naczelny Zaufanej Trzeciej Strony.
Adam opowie nam:
„Na co uważać dzisiaj i jutro – przegląd aktualnych zagrożeń”.
Kto wie, co jeszcze wydarzy się do 28.10

Marcin Tynda

Ethical Hacker | Audytor | Pentester

Temat przewodni wystąpienia Marcina to:
„Pentesterzy Offensive Security” w akcji, czyli etyczne hackowanie:
Przekraczając próg LABOR ZONE, wchodzisz na własną odpowiedzialność. To tutaj poznasz mroczne hakerskie sekrety.
-jak pozyskać dane metodami socjotechnicznymi
-jak znaleźć niezabezpieczone urządzenia IoT
-jak skopiować dane z kart
-bezpośrednie włamanie do hosta
Poznasz urządzenia do ataku i obrony przed włamaniami.

Dariusz Jakubowski

Rozmowa z Hackerem Celber

Ekstrawagancki haker pokaże jak i gdzie jesteś inwigilowany przez rządy i trzy literowe organizacje. Dowiesz się kilka porad jak nie dać się złapać.

zobacz więcej na: www.security.show.pancernik.it

PATRONAT
SECURITY MAGAZINE

PANCERNIK IT SECURITY SHOW 2022
TWORZYMY BEZPIECZNE IT

Fot. security.show.pancernik.it

Dołącz do nas i razem z nami twórz cyberbezpieczną społeczność!

Jesteśmy integratorem systemów IT działających w Polsce.
Oferujemy zaawansowane i innowacyjne rozwiązania z obszaru bezpieczeństwa IT sieci.

Mnogość czyhających zagrożeń w sieci sprawiła, że postawiliśmy sobie ambitny cel:

- edukowanie w temacie bezpieczeństwa IT,
- uświadamianie o cyfrowych niebezpieczeństwach,
- podpowiedź, jak stawiać im czoła.

Aby jak najlepiej realizować nasz plan, organizujemy Pancernikową konferencję poświęconą tematyce cyberbezpieczeństwa 28 października 2022 w Katowicach, Hotel Vienna House Easy.

Biorąc udział, zwiększysz swoją wiedzę i świadomość poprzez:

- Prelekcje najlepszych dostawców rozwiązań zwiększających bezpieczeństwo IT
- Aplikację szkoleniową VR
- Warsztaty techniczne
- Laboratorium
- Pentesty

Goście Specjalni:

- ADAM HAERTLE
- MARCIN TYNDA
- DARIUSZ JAKUBOWSKI CELBER

DLA CZYTELNIKÓW “SECURITY MAGAZINE” BONUS!
PODCZAS REJESTRACJI PODAJ KOD: IPV7
DZIĘKI TEMU WEJŚCIÓWKĘ NA WYDARZENIE OTRZYMASZ BEZPŁATNIE.
UWAGA! PROMOCJA DOTYCZY PIERWSZYCH 10 OSÓB, KTÓRE SKORZYSTAJĄ Z KODU.

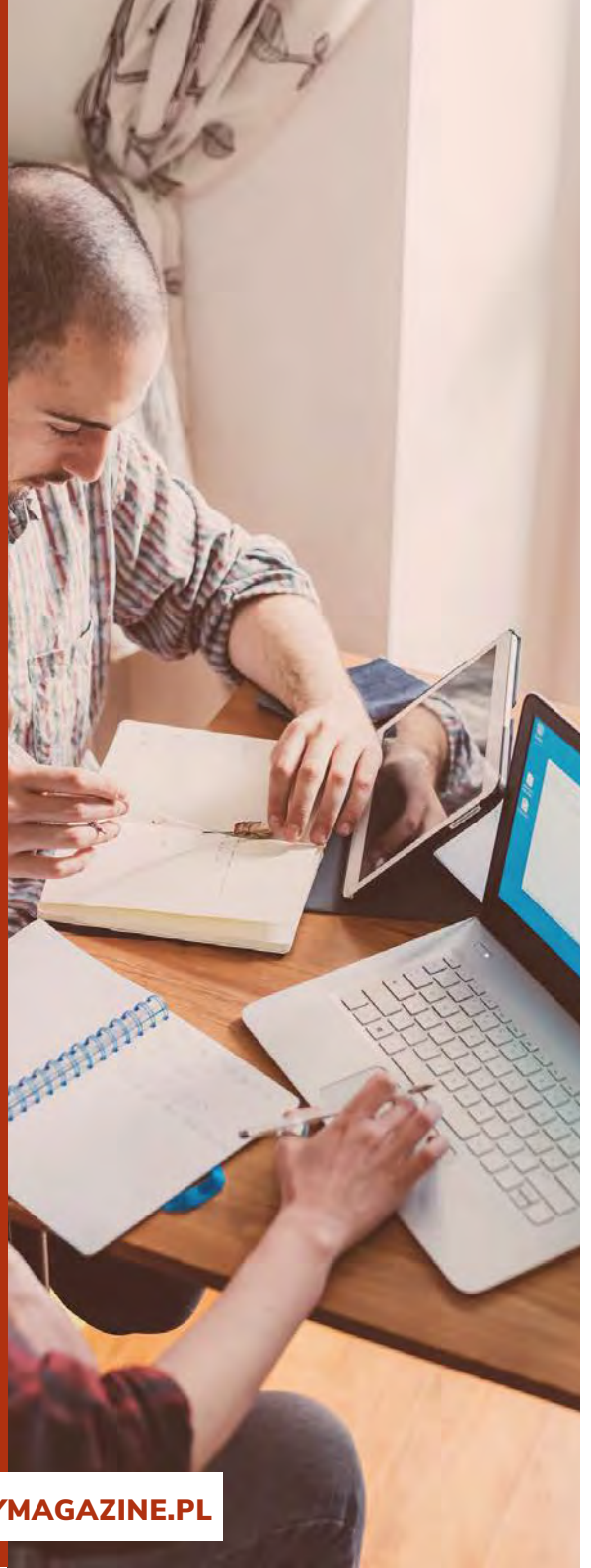
SECURITYMAGAZINE.PL

BEZPIECZNY KOMUNIKATOR, OBSŁUGA PŁATNOŚCI I UWIERZYTELNIANIE WIELOSKŁADNIKOWE

Redakcja
SECURITY MAGAZINE

#SECURITY
#STARTUP

Cyberbezpieczeństwo to szeroko zakrojony temat. W Polsce i na całym świecie funkcjonuje wiele startupów, które chronią przed zagrożeniami w sieci. I robią to na naprawdę wiele różnych sposobów. Sprawdź, jak kolejne trzy startupy pomogą Ci prowadzić bezpieczną cyfrowo firmę.



WETOG – BEZPIECZNY, KOMPLEKSOWY KOMUNIKATOR

Microsoft Teams, Slack, Mattermost – na rynku funkcjonuje wiele aplikacji ułatwiającej komunikację w firmie. Niektóre przedsiębiorstwa sięgają właśnie po te dedykowane platformy, inne przeprowadzają cały proces na „konsumenckich komunikatorach", jak np. Messenger czy WhatsApp. Jednak nie każda aplikacja zapewnia kompleksową obsługę i jest przy tym bezpieczna.

Utarło się, że najbezpieczniejszym komunikatorem jest Signal. I faktycznie to dość dobra oraz bezpieczna aplikacja. Jednak i ona musi mierzyć się z atakami hakerów, a ponadto niekoniecznie musi być wygodna do zarządzania komunikacją kilkudziesięcioosobowej firmy. A już tym bardziej jeszcze większej organizacji.

Alternatywę dla darmowych, jak i płatnych platform oferuje polskie WETOG. To aplikacja służąca zarówno jako komunikator, jak i usługa chmur. WETOG oferuje zarówno pisany czat, rozmowy wideo i umożliwia przechowywanie oraz szybkie udostępnianie plików (graficznych, wideo, tekstowych) czy danych. To tak, jakby połączyć Slacka z Mes-sengerem i Dyskiem Google. Dzięki czemu nie musisz tworzyć kont na kilku różnych aplikacjach – wystarczy korzystanie z jednej, komplek-sowej platformy.

Co ważne – wszystko od komunikacji pisemnej, przez wideo po usługę chmury jest szyfrowane.

WETOG działa w oparciu o autorski model LIQRYPT®, chroniący przed wyciekami. Startup chwali się, że większość zabezpieczeń używa 256-bitowego szyfrowania, które niejednokrotnie wykorzystuje zaledwie 16 bitów. Z kolei ich platforma ma działać na dwóch terabajtach szyfrowania, co oznacza różnorodne parametry o zmiennej długości klucza. Według startupu ze względu na to, że dodatkowe parametry kluczy nie są znane w całości, atak na dane zaszyfrowane przez LIQRYPT® zawsze kończy się niepowodzeniem.

SILENT EIGHT – BICZ NA FINANSOWYCH OSZUSTÓW

Silent Eight to międzynarodowy startup z polskim rodowodem, który jednak zarejestrowany jest w Singapurze. Spółka funkcjonuje od 2013 r. i doczekała się w tym czasie biur w Warszawie, Londynie, Nowym Jorku oraz we wspomnianym Singapurze. Silent Eight współpracuje przede wszystkim z bankami i fintechami, ale nic nie stoi na przeszkodzie, aby odpowiednio dostosować aplikację pod swoje wymagania.

Startup tworzy sztuczną inteligencję Iris, która wykorzystuje uczenie maszynowe. Jej funkcją jest wykrywanie nieprawidłowości w przepływie środków. Iris w zautomatyzowany sposób bada, skąd przepływają środki.

W ten sposób przeciwdziała praniu pieniędzy, finansowaniu terroryzmu czy transferu gotówki do krajów objętych sankcjami.

Spółka chwali się, że eliminuje ponad 80% fałszywych trafień dotyczących klientów i kontroli płatności, bez konieczności ludzkiej ingerencji. Ponadto monitoruje i automatyzuje cały proces weryfikacji transakcji, zmniejszając w ten sposób fizyczne wysiłki operacyjne o ponad 75%.

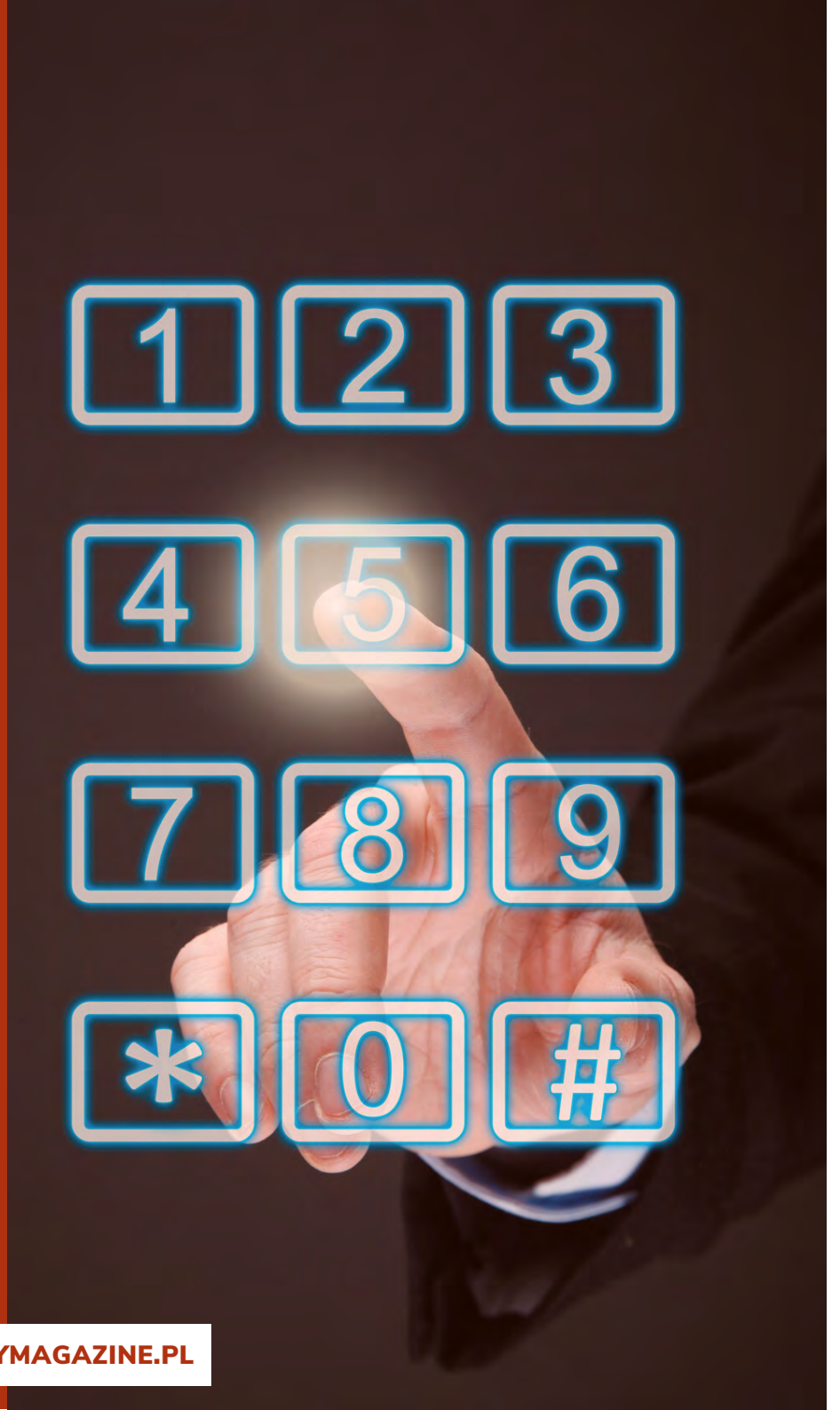
Sztuczna inteligencja stworzona przez Silent Eight obsługuje różne typy płatności, takie jak SWIFT, FEDWIRES, ACH, CHIPS i SEPA. Wspiera też podmioty w przejściu z płatności SWIFT MT na MX. W skrócie – Silent Eight znacząco zmniejsza ryzyko wszelkich nieprawidłowości związanych z transakcjami i weryfikuje płatników.

SECFENSE – UWALNIA FIRMY OD HASEŁ

Secfense to startup wywodzący się z Krakowa. Spółka dostarcza uwierzytelnianie wieloskładnikowe i jak sama się chwali – uwalnia w ten sposób firmy od haseł i to we wszystkich aplikacjach, z których korzysta. Secfense w szczególności zajmuje się wdrażaniem FIDO2, czyli globalnego standardu uwierzytelniania obejmującego np. czytniki biometryczne wbudowane w laptopy, smartfony czy tablety.

Startup oferuje jednak firmom zastosowanie także innych metody uwierzytelniania wieloskładnikowego. Mówiąc wprost – spółka pomaga zamieniać niewygodne używanie haseł i loginów na bezpieczniejsze, alternatywne metody. Mowa tu głównie o uwierzytelnianiu kryptograficznym, dzięki któremu dane uwierzytelniające są unikalne i nieprzechowywane na serwerach. Ma to eliminować ryzyko wycieku czy wyłudzania haseł np. za pomocą phishingu.

Takie uwierzytelnianie działa na podstawie czytników linii papilarnych czy twarzy. Alternatywą są klucze bezpieczeństwa FIDO, które wkłada się do portów USB. Wszelkie witryny internetowe mogą wykorzystywać tę metodę za pomocą prostego wywołania interfejsu API JavaScript. Dzięki temu można wyeliminować konieczność wpisywania haseł w którejkolwiek z aplikacji.



Secfense podkreśla, że w ten sposób można chronić całą organizację. A co więcej – jakiekolwiek zmiany aplikacji nie wpływają na działanie ich technologii. Klientami Secfense są już m.in. PKP Intercity czy bank BNP Paribas Polska.

Jak widać, startupy mogą zapewnić ochronę w cyfrowym świecie na wiele różnych sposobów. Od bezpiecznej komunikacji, przez logowanie się bez haseł po weryfikację płatników.

PATRONAT
SECURITY MAGAZINE

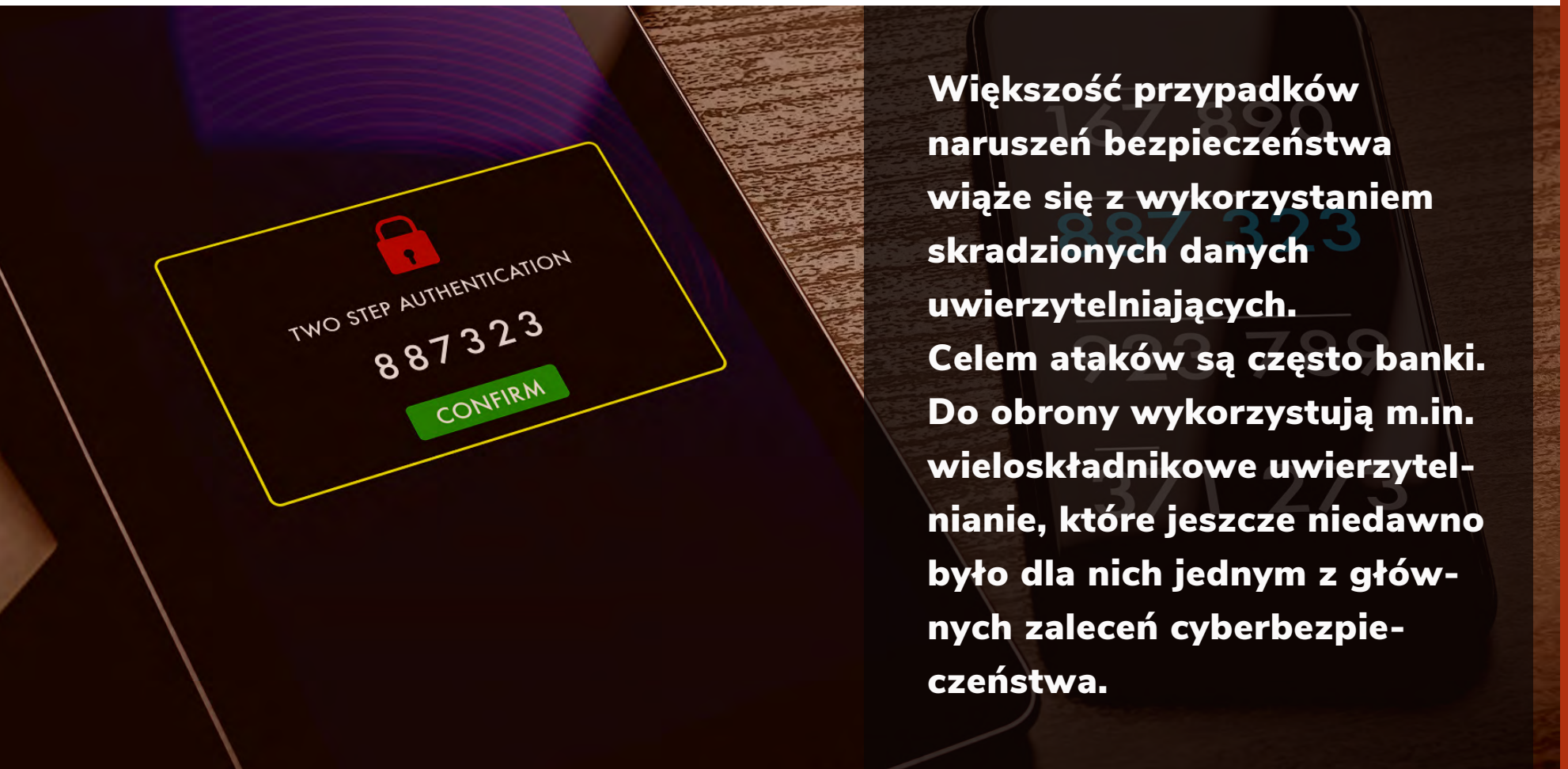
13-14 października w Rzeszowie na arenie do walki o inwestora staną startupy, scaleupy i ludzie z nietuzinkowymi pomysłami na biznes. Podczas drugiej edycji #CSF22 Carpathian Startup Fest 2022 będzie też mowa o zastosowaniu sztucznej inteligencji, występy czołowych postaci polskiego środowiska startupowego, spotkania z inwestorami, targi pracy branży technologicznej oraz strefa wystawiennicza dla startupów.

Podczas #CSF22 zaprezentują się 24 najlepsze projekty wybrane spośród 226 zgłoszeń na festiwal. Do wygrania jest łącznie 100 tys. zł oraz zaproszenie do udziału w programie dla najbardziej innowacyjnych startupów **InCredibles zainicjowanym przez Sebastiana Kulczyka**. Będzie także specjalna nagroda od RARR dla startupu z Ukrainy. Festiwal startupów to nie tylko konkurs dla tych, którzy przeszli eliminacje, ale wydarzenie dla wszystkich zainteresowanych nowymi technologiami i najnowszymi trendami w biznesie. Zaplanowano mnóstwo wydarzeń towarzyszących.

Podczas 2 dni festiwalowych wystąpią m.in.: **Stefan Batory, współzałożyciel i prezes Booksy, Michał Sadowski, założyciel i prezes zarządu Brand24, czy Katarzyna Cichopek, właścicielka marki Yacichopek.pl.**

GLOBALNY PROBLEM Z MFA

Tomasz Kowalski
Secfense



Większość przypadków naruszeń bezpieczeństwa wiąże się z wykorzystaniem skradzionych danych uwierzytelniających. Celem ataków są często banki. Do obrony wykorzystują m.in. wieloskładnikowe uwierzytelnianie, które jeszcze niedawno było dla nich jednym z głównych zaleceń cyberbezpieczeństwa.

W Polsce, jak podaje raport ZBP InfoDok, tylko w I kwartale 2022 roku oszuści podjęli 1915 prób kradzieży z wykorzystaniem przejętych danych osobowych, w sumie na kwotę 575 tys. zł. To średnio aż 21 wyłudzeń dziennie. **Banki i instytucje finansowe są jednym z głównych wektorów takich ataków.**

Według raportu The State of Authentication aż 80% z nich doznało przynajmniej jednego naruszenia danych w ciągu ostatnich 12 miesięcy, a phishing był najbardziej rozpowszechnionym zagrożeniem, stanowiąc 36% wszystkich incydentów. Jednym z powodów nasilających się zagrożeń tego typu jest niewystarczająca ochrona tożsamości użytkowników.

ŚWIATOWY PROBLEM

Jeszcze kilka lat temu znana wszystkim technologia 2FA lub MFA (dwu- lub wieloskładnikowe uwierzytelnianie) uchodziła za jedną z najbardziej skutecznych metod ochrony użytkowników w sieci. Dziś jednak wyrafinowani intruzi znaleźli sposoby, aby również i te zabezpieczenia skutecznie obchodzić.

Globalnym wyzwaniem drugiej dekady dwudziestego pierwszego wieku pozostaje nie samo MFA, a wysoki poziom skomplikowania i różnorodności środowisk IT oraz implementacja w nich skutecznych metod wieloskładnikowego użytkowania.

Z tego powodu w wielu dużych organizacjach większość systemów i aplikacji albo nie jest zabezpieczona MFA, albo jest chroniona przestarzałymi metodami, takimi jak SMS czy kody TOTP, które nie bronią nas przed nowoczesnymi atakami typu phishing.

TYLKO FIDO2

Według badania firmy HYPR Report: State of Authentication in the Finance Industry 2022, 32% pracowników banków z USA (200 osób ankietowanych), Wielkiej Brytanii (100 osób), Francji (100 osób) i Niemiec (100 osób) nadal korzysta z tradycyjnych i przestarzałych już metod MFA, takich jak SMS-y i hasła jednorazowe. 43% pytanych polega na menedżerach haseł, a 22% polega wyłącznie na nazwach użytkowników i hasłach.

I jeśli faktycznie kilka lat temu uwierzytelnianie wieloskładnikowe było de facto zaleceniem cyberbezpieczeństwa dla firm i banków, to dziś jedynym rozwiązaniem, w pełni odpornym na phishing oraz kradzież loginów i haseł, jest otwarty i darmowy standard uwierzytelniania FIDO2.

Pozwala on na wykorzystanie kluczy kryptograficznych, ale również urządzeń, które zawsze mamy przy sobie, takich jak laptopy z wbudowaną kamerą, Windows Hello lub smartfony z czytnikiem linii papilarnych, stosowane w celu potwierdzenia tożsamości w sieci.

NIEWYKORZYSTANE BEZPIECZEŃSTWO

Zdanie specjalistów od bezpieczeństwa IT potwierdzają również osoby na co dzień pracujące w zbadanych przez HYPR instytucjach finansowych. Aż 99% ankietowanych osób przyznało, że metody uwierzytelniania stosowane w ich organizacjach wymagają unowocześnienia.

Taki proces modernizacji jednak nie jest aktualnie możliwy. Dlaczego? Ponieważ stoją mu na przeszkodzie m.in. problemy z posiadanymi przez firmy systemami informatycznymi (75%), w tym złożone nimi zarządzanie (33%) i trudności związane z integracją (27%).

Te wyniki badań dokładnie odzwierciedlają również polską rzeczywistość, bo faktycznie największy kłopot wciąż sprawia implementacja wieloskładnikowego uwierzytelniania.

Wdrożenie MFA jest trudne, uciążliwe i kosztowne. Jeśli bank posiada w swojej infrastrukturze IT setki aplikacji, a tak jest w większości dużych organizacji, masowa implementacja na wszystkich programach jest praktycznie niewykonalna.

Efekt? Jedna z najlepszych metod uwierzytelniania, czyli standard FIDO2 – choć zaprojektowany już w kwietniu 2018 – po ponad czterech latach wciąż jest jeszcze dodatkiem, a nie uniwersalnym sposobem zabezpieczania tożsamości w Internecie.

REWOLUCJA ZA DARMO

Metoda FIDO2 zrewolucjonizowała podejście do bezpiecznego uwierzytelniania w sieci. FIDO2 to otwarty standard, dzięki któremu każda usługa w Internecie może zostać dziś zabezpieczona w pełni odpornym na phishing i kradzież haseł uwierzytelnianiem.

Jak obejść więc problem z implementacją MFA opartą na FIDO2 w skomplikowanych środowiskach IT? Jedyną drogą jest wykorzystanie dobrodziejstwa technologii, która umożliwi aktywację usług związanych z podniesieniem poziomu bezpieczeństwa w procesie uwierzytelniania użytkowników oraz autoryzacji kluczowych transakcji w dowolnej aplikacji web.

Wymyślone przez Secfense rozwiązanie User Access Security Broker buduje warstwę ochronną, następnie polityki bezpieczeństwa egzekwuje “w locie”, bez bezpośredniej ingerencji w chronione aplikacje.

Technologia UASB została tak zaprojektowana, by w warunkach “zerowej” wiedzy o aplikacjach i środowisku informatycznym, które ma chronić, była zdolna nauczyć się go i zrozumieć procesy logowania użytkowników aplikacji.

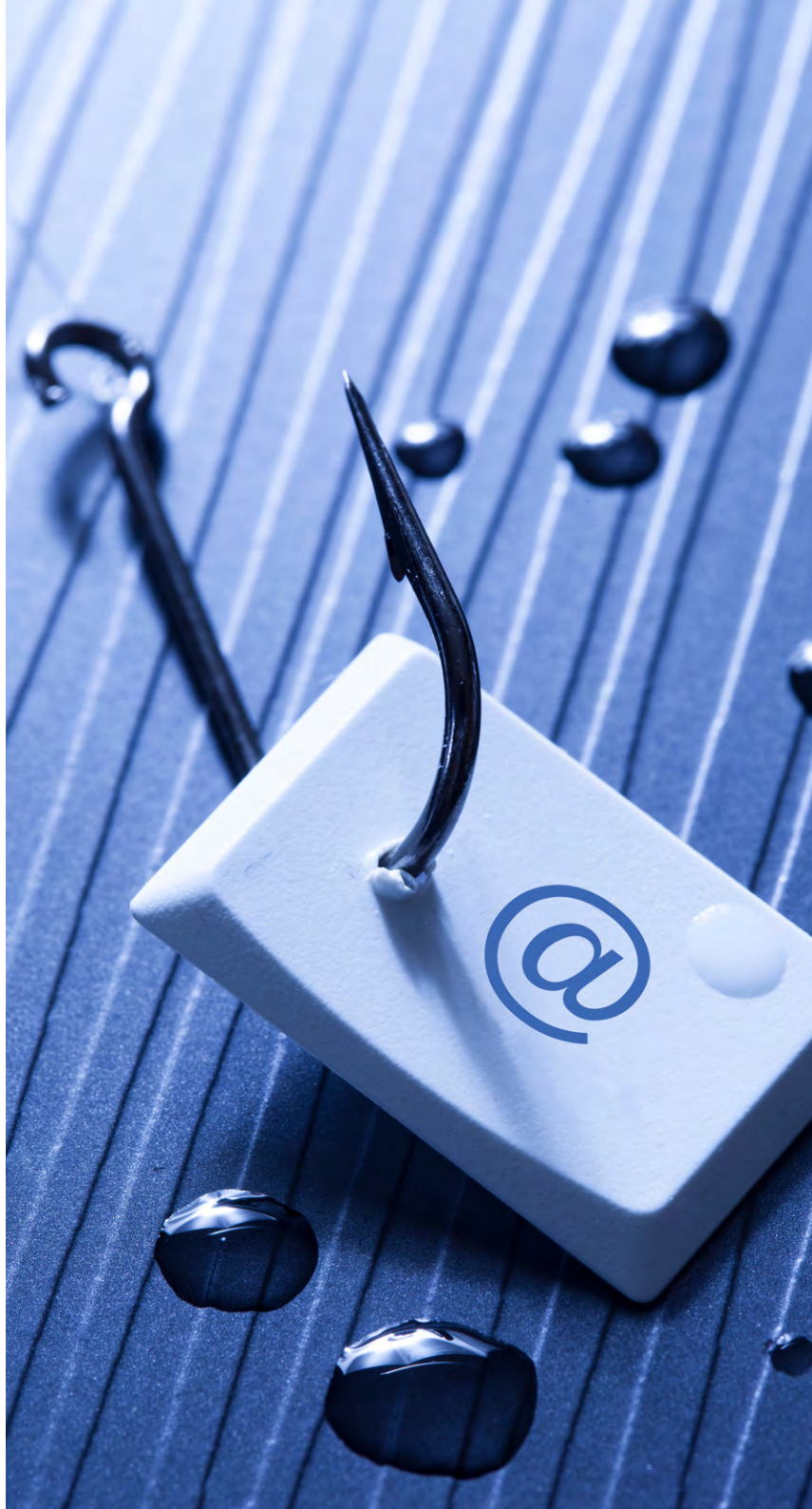
Etap uczenia się, podczas którego UASB uruchamia sondę do docelowej aplikacji, rejestruje wzorce logowania użytkownika, którego konto ma być chronione uwierzytelnianiem FIDO2. W kolejnym kroku wzorce te są aktywowane i przy każdym następnym logowaniu użytkownik jest proszony o potwierdzenie swojej tożsamości. Spogląda w kamerę, skanuje swoją twarz lub przykłada palec, dokładnie tak samo, jak do tej pory logował się do swojej stacji roboczej.

ZERO ZAUFANIA

Na rynku istnieje wiele rozwiązań z zakresu cyberbezpieczeństwa, które chronią przed różnymi wektorami ataków. Aktualnie jednak za najwygodniejsze i najskuteczniejsze uznaje się uwierzytelnianie bez hasła (**passwordless authentication**). Niestety, temat nadal jest często ignorowany w praktyce.

Na szczęście – jak mówią wyniki badania HYPR – większość respondentów wierzy, że bezhasłowe uwierzytelnianie jest najlepszą metodą ochrony. Aż 89% z nich twierdzi, że zwiększa stanowczo bezpieczeństwo i zadowolenie użytkowników. A czy właśnie nie o te wartości najbardziej nam wszystkim chodzi?

Pewne jest, że żadna sieć firmowa nie jest bezpiecznym zamkiem, do którego nie mają dostępu osoby z zewnątrz. Przeciwnie, rosnąca liczba aplikacji w chmurze, praca z domów i z niezabezpieczonych odpowiednio sieci sprawia, że każdą osobę, która pojawia się w naszej sieci, musimy traktować jak intruza.



Takie założenie to podstawa modelu Zero Trust, który odpowiednio obsługuje i wspiera pracę zdalną oraz zapewnia bezpieczeństwo ludzi, urządzeń, aplikacji niezależnie od miejsca.

Ale aby Zero Trust działał naprawdę, nie wystarczy wprowadzenie przypadkowego MFA tylko w najważniejszych systemach i aplikacjach. Warunkiem koniecznym jest zabezpieczenie całej organizacji odpornym na phishing standardem FIDO i wdrożenie go globalnie, najlepiej w sprawny i zautomatyzowany sposób.

Tylko wtedy, kiedy na 100% wiemy, kto siedzi po drugiej stronie monitora, możemy być pewni, że organizacja chroniona jest w wystarczający sposób.

CO BIZNES MUSI WIEDZIEĆ O PROCESACH KRYTYCZNYCH?

Renata Davidson
Davidson Consulting

„Cóż to za dziwne pytanie o procesy krytyczne? Przecież wiadomo, że wszystko jest krytyczne, a najbardziej sprzedaż. Poza tym, kiedyś opracowaliśmy listę procesów i nic nam to nie dało” – takie lub podobne stwierdzenie można usłyszeć stosunkowo często w odpowiedzi na pytanie o procesy krytyczne. Jeszcze trudniejsze okazuje się pytanie o krytyczne systemy IT, ale to już temat na osobny artykuł.

Intuicja podpowiada przedsiębiorcom, że procesy krytyczne to zwykle te, od których zależą przychody firmy i intuicja zwykle przedsiębiorców nie myli, ale też i nie umożliwia uzyskania pełnego obrazu. W celu prawidłowej identyfikacji procesów krytycznych dobrze jest sięgnąć do sprawdzonych narzędzi z obszaru zarządzania ciągłością działania (z ang. Business Conitnuity Management, BCM).

Możemy z powodzeniem założyć, że żadna organizacja, zwłaszcza przedsiębiorstwo, nie realizuje procesów „zbędnych", a każda z aktywności może okazać się krytyczna w zależności od aktualnej sytuacji w otoczeniu wewnętrznym lub zewnętrznym. Dlatego też obecnie odchodzi się od tego pojęcia lub stosuje się je jako określenie potoczne, a w zamian coraz częściej mówi się o „procesach upriorytetyzowanych" lub - zgodnie z zasadami języka polskiego - o „procesach, którym nadano priorytety".*

Z równie dużą dozą pewności możemy też przyjąć, że każdy z procesów może otrzymać zupełnie różne priorytety w zależności od tego, kogo o nie zapytamy – dlatego przed przystąpieniem do ich identyfikacji należy określić uniwersalne i jak najbardziej obiektywne, mierzalne kryteria.

Nie chodzi o podważanie wiedzy i doświadczenia właścicieli procesów – wszak to oni są ekspertami w swoich dziedzinach, chcę natomiast zwrócić Państwa uwagę na to, że aby wyznaczyć priorytety dla wielu zupełnie różnych procesów, należy je w jakiś sposób porównać i wtedy dobrze jest stosować do wszystkich jednakową miarę.

Co może zatem stanowić taką obiektywną miarę, skoro nie wszystkie procesy przynoszą nam przychody, a niektóre realizujemy z konieczności i są one dla nas źródłem kosztów, a czasem nawet organizacyjnym utrapieniem?

Takim wspólnym mianownikiem bez wątpienia jest poziom **negatywnego** wpływu, na jaki byłaby narażona organizacja, gdyby doszło do niespodziewanej przerwy w realizacji danego procesu i to w najgorszym możliwym momencie.

** W punkcie 3.25 polskiej PN-EN ISO 22301:2020, dotyczącej zarządzania ciągłością działania znajduje się niezbyt szczęśliwie przetłumaczone pojęcie „działanie priorytetowe", które zyskuje coraz większą popularność.*

Jednym zdaniem: nie każdy proces generuje przychody, ale każdy proces może przynieść straty (finansowe, wizerunkowe, negatywne skutki prawne), jeśli przerwiemy go na wystarczająco długi czas. I to właśnie ten czas trwania przerwy stanowi główny wskaźnik dla wyznaczania priorytetu procesu.

Prawidłowo przeprowadzona analiza wpływu zdarzenia na organizację (z ang. Business Impact Analysis, analiza BIA) dostarcza wszystkich informacji niezbędnych do określenia maksymalnego dopuszczalnego czasu trwania przerwy, a tym samym do wyznaczenia priorytetów dla poszczególnych procesów.

Rzecz jasna, priorytet wyznaczony w ten sposób oznacza przede wszystkim priorytet dla odtworzenia procesów, ale niewątpliwie jest to wskaźnik uniwersalny, umożliwiający porównywanie procesów między sobą i, co równie ważne, porównywanie priorytetów procesów między kolejnymi iteracjami analizy BIA w kolejnych latach i obserwowanie trendów.

Za zastosowaniem analizy BIA do wyznaczania priorytetów dla procesów przemawiają również względy prawne, w przypadkach, w których zgodnie z wymaganiami ustawowymi** przedsiębiorstwo jako operator usługi kluczowej i tak jest zobowiązane do za-

** *Np. Ustawa z dnia z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.*

pewnienia ciągłości działania dla wszystkich lub wybranych produktów i usług, lub gdy nasza firma jest dostawcą dla takiego operatora usługi kluczowej.

Podstawowy zasób informacji, który warto zebrać dla każdego procesu to:

1. **lista osób i organizacji** (interesariuszy zewnętrznych i wewnętrznych), które stawiają wymagania jakościowe, ilościowe, terminowe wobec danego procesu lub produktów i usług, które ten proces dostarcza,
2. **lista wymagań,** a także nieformalnych oczekiwań interesariuszy,
3. **lista wymagań prawnych** wobec każdego procesu,
4. **potencjalne skutki** (finansowe i niefinansowe), jakie może przynieść niedotrzymanie wymagań, o których mowa w pkt. b) i c) (przyjmując pesymistyczne założenia, aby oszacować maksymalny potencjalny wpływ),
5. **maksymalny dopuszczalny czas** trwania przerwy w spełnianiu wymagań (czas, jaki może upłynąć zanim skutki staną się nieakceptowalne),
6. **minimalny poziom realizacji procesu** w sytuacji kryzysowej, w tym wymagania dotyczące dostępności danych,
7. **maksymalny czas**, po upływie którego proces musi wrócić do normalnego poziomu,
8. **zasoby niezbędne do realizacji** danego procesu **na normalnym poziomie**,
9. **zasoby niezbędne do realizacji procesu na minimalnym poziomie**, o którym mowa w pkt. f),
10. **zagrożenia,** które mogą spowodować niedotrzymanie wymagań, o których mowa w pkt. b) i c),
11. **środki kontroli, zabezpieczenia,** które mogą ograniczyć szansę wystąpienia, zakres lub poziom negatywnego wpływu wystąpienia zagrożeń, o których mowa w pkt. j).

PO CO ORGANIZACJI TAKI ZESTAW INFORMACJI?

Otóż, tylko na ich podstawie można w obiektywny sposób wyznaczyć priorytety dla procesów (szczególnie na podstawie pkt. d)), oszacować ekspozycję na ryzyko wystąpienia negatywnych skutków i przygotować adekwatne plany postępowania z tym ryzykiem.

Potencjalna maksymalna strata oszacowana podczas analizy BIA stanowi obiektywny punkt odniesienia podczas podejmowania decyzji o dodatkowych zabezpieczeniach, w tym o kosztownych inwestycjach w infrastrukturę techniczną.

I tu dochodzimy do odpowiedzi na pytanie, co o procesach krytycznych musi wiedzieć IT, a także wszystkie inne obszary techniczne, wspierające realizację procesów biznesowych?

Zakres informacji, który powinno otrzymać IT i inne obszary techniczne w zasadzie zawiera się w punktach od e) do i) powyżej, natomiast w przypadku atrybutu dostępności należy pamiętać o dodatkowym wskaźniku, jakim jest punkt odtworzenia danych (z ang. Recovery Point Objective, RPO), innymi słowy: czy zgadzamy się na utratę danych (RPO > 0) i z jakiego okresu, licząc wstecz od chwili wystąpienia incydentu. Na przykład RPO = 2h oznacza, że zgadzamy się na utratę danych z ostatnich dwóch godzin sprzed zdarzenia, a RPO = 24h oznacza w uproszczeniu, że wystarczający będzie dostęp do danych z poprzedniego dnia.

Po otrzymaniu od właścicieli procesów informacji o minimalnym zakresie niezbędnych zasobów technicznych (punkt i)), komórki organizacyjne odpowiedzialne za ich utrzymanie powinny wykonać analizę zasobów, które są im potrzebne do spełnienia wymagań biznesowych w punktach e) - g) i przeanalizować zagrożenia, które mogłyby spowodować ich niedostępność lub nieprawidłowe funkcjonowanie (w zależności od obszaru, w którym dokonujemy analizy wpływu).

Dopiero na tej podstawie obszar IT może ocenić poziom gotowości do spełnienia wymagań biznesowych, rekomendacje dodatkowych zabezpieczeń lub rozwiązań zapasowych, strona biznesowa i usługodawcy wewnętrzni i zewnętrzni mogą uzgodnić SLA w oparciu o obiektywne kryteria wynikające z analizy BIA, a właściciele procesów biznesowych mogą podjąć świadomą decyzję (well-informed decision) dotyczącą ewentualnych zmian w sposobie realizacji procesów (działania mitygujące), inwestycji w dodatkowe zabezpieczenia lub akceptacji ryzyka.

Analiza wpływu znajduje zastosowanie nie tylko w przypadku zarządzania ciągłością działania. Jest to pierwszy krok w procesie oceny i szacowania ryzyka każdego rodzaju.

Na przykład, w zarządzaniu bezpieczeństwem informacji szacujemy potencjalny wpływ naruszenia poszczególnych atrybutów, a następnie oceniamy szansę wystąpienia tych naruszeń. W tym samym obszarze analizujemy potencjalny wpływ naruszenia ochrony szczególnego typu informacji, jakim są dane osobowe, na osoby, których dane dotyczą (analiza PIA).

Tam, gdzie możemy zastosować analizę wpływu (a po drobnych korektach możemy zastosować ją w zasadzie wszędzie), możemy wykorzystać jej wyniki do zwiększenia poziomu bezpieczeństwa organizacji (fizycznego, cyberbezpieczeństwa, prawnego, finansowego), ograniczyć ryzyko wystąpienia nieakceptowalnych strat, a ponadto zwiększyć transparentność procesu decyzyjnego dotyczącego inwestycji w zabezpieczenia i w nowe rozwiązania.

Dzięki wynikom analizy BIA, na etapie projektowania nowych rozwiązań informatycznych, technicznych i organizacyjnych można uwzględnić priorytety wynikające z procesów, które będą z nich korzystać i umieścić w projekcie środki kontroli – zgodnie z podejściem opartym na ryzyku (risk based approach), podejściem „secure by design" czy „privacy by design".

Wiarygodna informacja dotycząca priorytetów procesów biznesowych może być wykorzystywana do podejmowania strategicznych decyzji w organizacji. To z tego powodu przeczucie lub opinia ekspercka nie powinny stanowić jedynego kryterium oceny krytyczności procesu.

Wiele organizacji boleśnie przekonało się o prawdziwości powiedzenia: **„Nie możesz zmienić czegoś, czego nie widzisz"**. Do analizy wpływu niezbędne jest posiadanie choćby najprostszej, ale prawidłowo zdefiniowanej i wdrożonej architektury procesów. Dzięki niej możemy widzieć organizację na przestrzał – wszystkie powiązania, zależności, wykorzystywane zasoby, szanse i zagrożenia. Taka architektura, stanowi kanwę, na której można planować, modelować i skutecznie wdrażać wszelkie zmiany oraz świadomie zarządzać ryzykiem, zręcznie unikając nieakceptowalnych skutków i umiejętnie wykorzystując nadarzające się szanse.

Mam nadzieję, że artykuł stanie się źródłem inspiracji do doskonalenia systemów zarządzania w organizacjach i że pokusicie się Państwo o wdrożenie analizy wpływu jako podstawowego narzędzia do wyznaczania priorytetów, oceny ryzyka i podejmowania decyzji.

DAVIDSON CONSULTING

Porozmawiajmy o ryzyku

- Zarządzanie Ciągłością Działania
- Analiza BIA
- Zarządzanie Ryzykiem Operacyjnym
- Zarządzanie Zgodnością (Compliance)
- Cyberbezpieczeństwo (UKSC)
- Disaster Recovery

Połączmy się przez LinkedIn

BEZPIECZEŃSTWO W SIECI. OBALAMY MITY

Kris Durski
Vault Security

Każdy, kto posiada lub zarządza cennymi aktywami, cyfrowymi lub materialnymi i chce umożliwić dostęp do nich innym, nawet, jeśli jest to niewielka grupa ludzi, zadaje sobie pytanie: w jaki sposób mogę zapewnić, że te aktywa nie trafią w złe ręce? To wtedy musimy zdać sobie sprawę, że urządzenia lub oprogramowanie nie popełniają przestępstw, ale ludzie to robią.

LUDZIE O ZŁYCH INTENCJACH

Ludzie mogą być najbardziej narażeni w całej operacji lub najbardziej groźni, w zależności od tego, po której stronie się znajdują. W praktyce jednak musimy założyć, że oprogramowanie, jak i sprzęt mogą być złośliwe, nawet, jeśli zostały pozyskane z legalnego źródła. Za tym zawsze stoją ludzie o złych intencjach, którzy potrafią znaleźć drogę do wytyczonego celu.

Przyjrzyjmy się wszystkim tym miejscom, w których ludzie najmniej spodziewają się problemów z zabezpieczeniem swoich aktywów i mam na myśli nie tylko zwykłych śmiertelników, ale także ekspertów. Istnieje tendencja, aby bardziej ufać sprzętowi niż oprogramowaniu i jest ku temu uzasadniony powód. Podczas gdy oprogramowanie może tworzyć praktycznie każdy, kto nabył pewne umiejętności, to rozwój i produkcja sprzętu wymaga zwykle bardzo kosztownej infrastruktury.

Ponadto oprogramowanie może zostać poprawione po jego wydaniu, podczas gdy każdy problem sprzętowy wymaga powtórzenia całego procesu rozwoju i zaangażowania w jego produkcję.

Z tego powodu funkcjonowanie sprzętu jest również kontrolowane przez wbudowane oprogramowanie, które można również w razie potrzeby poprawić bez tego kosztownego procesu projektowania i produkcji. Pewnie już widzicie, dokąd zmierzam.

Zaufane urządzenie może zostać zhakowane tak samo jak oprogramowanie. To tam wychodzi na jaw jailbreak*, cracking** lub rootowanie***. Chociaż wielu producentów uważa to za złamanie umowy licencyjnej użytkownika końcowego, czasami może to być zrobione z powodów pirackich, co jest znacznie większym przestępstwem niż nieprzestrzeganie umowy licencyjnej. Tak więc, z punktu widzenia bezpieczeństwa, umowa licencyjna użytkownika końcowego nigdy nie powinna być traktowana jako środek odstraszający zainteresowanych zhakowaniem urządzenia.

Usuwa niektóre środki bezpieczeństwa firmy Apple, dzięki czemu Twoje urządzenie staje się podatne na złośliwe oprogramowanie i naruszenia bezpieczeństwa danych.

***Technika wykorzystywana do włamywania się do oprogramowania komputerowego lub całego systemu bezpieczeństwa komputerowego, która ma na celu szkodzić istniejącemu układowi.*

****Usuwa niektóre środki bezpieczeństwa systemu Android oraz innych opartych na Linux.*

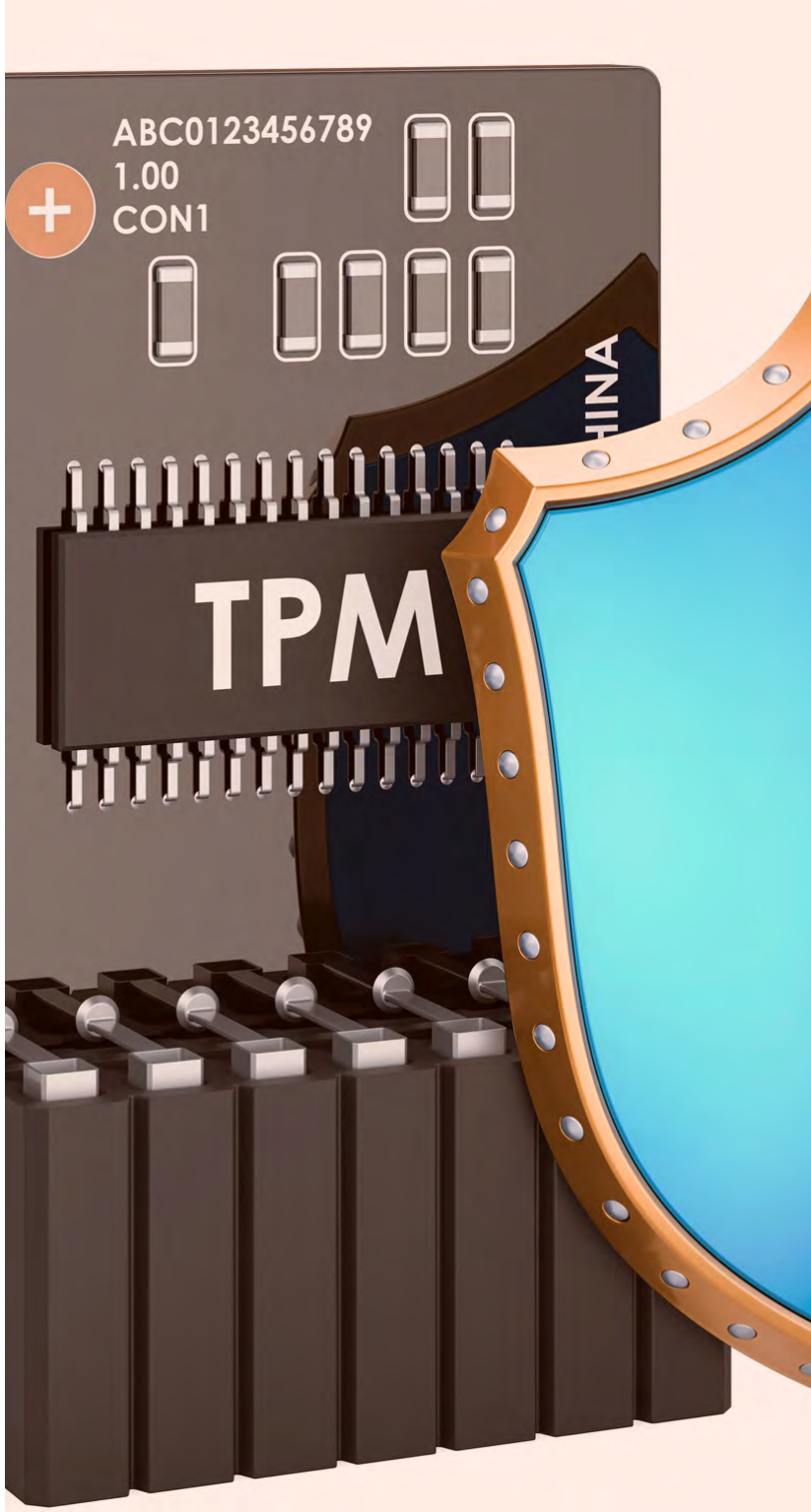
CHIP ZABEZPIECZAJĄCY

Innym problemem jest przekonanie, że TPM (Trusted Platform Module) czasami nazywany chipem zabezpieczającym, nigdy nie wypuszcza kluczy prywatnych poza swoje granice, więc klucze te są dobrze chronione przez sprzęt elektroniczny w jego wnętrzu.

Jednak zawsze musi istnieć możliwość tworzenia kopii zapasowych na wypadek awarii urządzenia i konieczności przywrócenia kluczy na innym urządzeniu. Właśnie tam są słabe punkty. Ponadto TPM to nie to samo, co HSM (Hardware Security Module), który działa w znacznie bezpieczniejszym środowisku, ale ma również słabe punkty z kopiami zapasowymi.

Aby mieć jasność, co do modułów bezpieczeństwa, musimy podkreślić fakt, że klucze szyfrowania nigdy nie są celem hakerów. W kluczach nie ma nic wartościowego. Celem są zasoby, które są chronione tymi kluczami, więc jeśli istnieje możliwość korzystania z kluczy bez ich posiadania, ochrona nie istnieje pomimo sprzętowej enkapsulacji.

Powszechnym błędem jest niedocenianie „czynnika przyjaznego dla człowieka” we wszystkich cyberwłamaniach i przywiązywanie nadmiernej wagi do problemów ze sprzętem lub oprogramowaniem. Widać to w przypadku sojuszu FIDO (Fast Identity Online), w którym certyfikacja urządzenia i jego atestacja są w najwyższym stopniu ukierunkowane na zapewnienie dobrego bezpieczeństwa. Czy sprawca może kupić certyfikowane urządzenie i użyć go do popełnienia przestępstwa? Na pewno nic tego nie zabrania. Tak jak przestępcy mogą legalnie kupować broń, mogą również kupować certy-

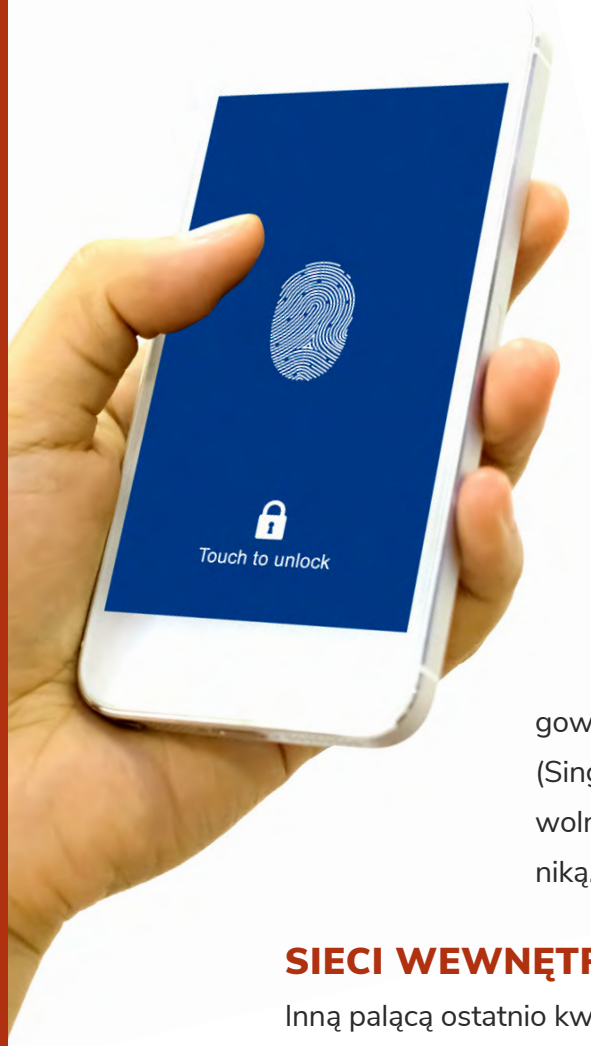


fikowane urządzenia elektroniczne, aby używać ich „legalnie” do popełniania przestępstw.

KLUCZ DO BEZPIECZEŃSTWA

Jak wspomniałem wcześniej, jeśli jest przestępstwo, to zawsze stoi za tym człowiek, więc włączenie czynnika ludzkiego jest kluczem do dobrego bezpieczeństwa. Wszyscy wiemy, że używanie hasła do uwierzytelnienia osoby powinno być reliktem przeszłości. Jednak przejście w kierunku biometrycznego odblokowania urządzenia jako kluczowy czynnik bezpieczeństwa jest dużym błędem w uwzględnieniu czynnika ludzkiego. Troska o prywatność nie powinna być wymówką do ignorowania osoby, która faktycznie korzysta z urządzenia, zwłaszcza, jeśli dane osobowe zostały już zebrane w celu otwarcia konta umożliwiającego korzystanie z usługi.

Prawdziwe bezpieczeństwo uprawnionych użytkowników jest tak naprawdę ignorowane, a obecne działania dają więcej korzyści hakerom. FIDO rejestrują urządzenie, a zarejestrowany login i hasło właściciela konta zastępują danymi biometrycznymi, które są przechowywane na urządzeniu oraz hasłem, którego nazwa została zmieniona na kod/pin, który także jest przechowywany na urządzeniu do wykorzystania w przypadku, gdy autoryzacja za pomocą danych biometrycznych nie powiedzie



się. Czy sprawca może podszyć się pod legalnego użytkownika? Odpowiedź brzmi - **tak**. Dodatkowo uwierzytelnianie nie jest bezhasłowe, jak jest szeroko reklamowane, ale logowanie jednokrotne (Single-Sign-On) z dowolną dostępną techniką.

SIECI WEWNĘTRZNE

Inną palącą ostatnio kwestią jest potrzeba poprawy bezpieczeństwa sieci wewnętrznych poprzez zastąpienie organizacyjnego bezpieczeństwa obwodowego zwiększoną granularnością sieci podzielonej na mniejsze niezależne podsieci nazywane ZTA (Zero Trust Architecture) lub ZTN (Zero Trust Network). Zmniejsza to ewentualne korzyści hakera w przypadku naruszenia, ponieważ tylko jedna komórka lub podsieć może zostać spenetrowana za pomocą pojedynczego ataku. Jeśli docelowy zasób jest rozłożony na wiele komórek, sprawca musi być przygotowany na wiele działań hakujących, co znacznie zwiększa koszty i czas - szczęśliwie dla właściciela sieci, nieopłacalne dla hakera.

Duża szczegółowość sieci to nie tylko ból głowy dla hakerów, ale także dla jej użytkowników. Nagle muszą przełączyć się z jednego konta na wiele. Wielokrotne użycie tego samego hasła zniweczy cały cel owej architektury, a tym samym zmarnuje inwestycję bez poprawy bezpieczeństwa. Z drugiej strony proszenie użytkowników o zapamiętanie dużej liczby haseł jest nie tylko nierozsądne, ale także niewykonalne.

SSO

Jednak kolejne rozwiązanie, które staje się obecnie modne i powszechnie używane, jest tak samo bezużyteczne, jak powtarzające się hasła. Zarządzanie dostępem, umożliwia użytkownikom dostęp do wielu podsieci za pomocą jednego logowania (Single-Sign-On inaczej SSO). Brzmi to jak genialne rozwiązanie, ale jest sprzeczne z celem pierwotnych założeń polega-

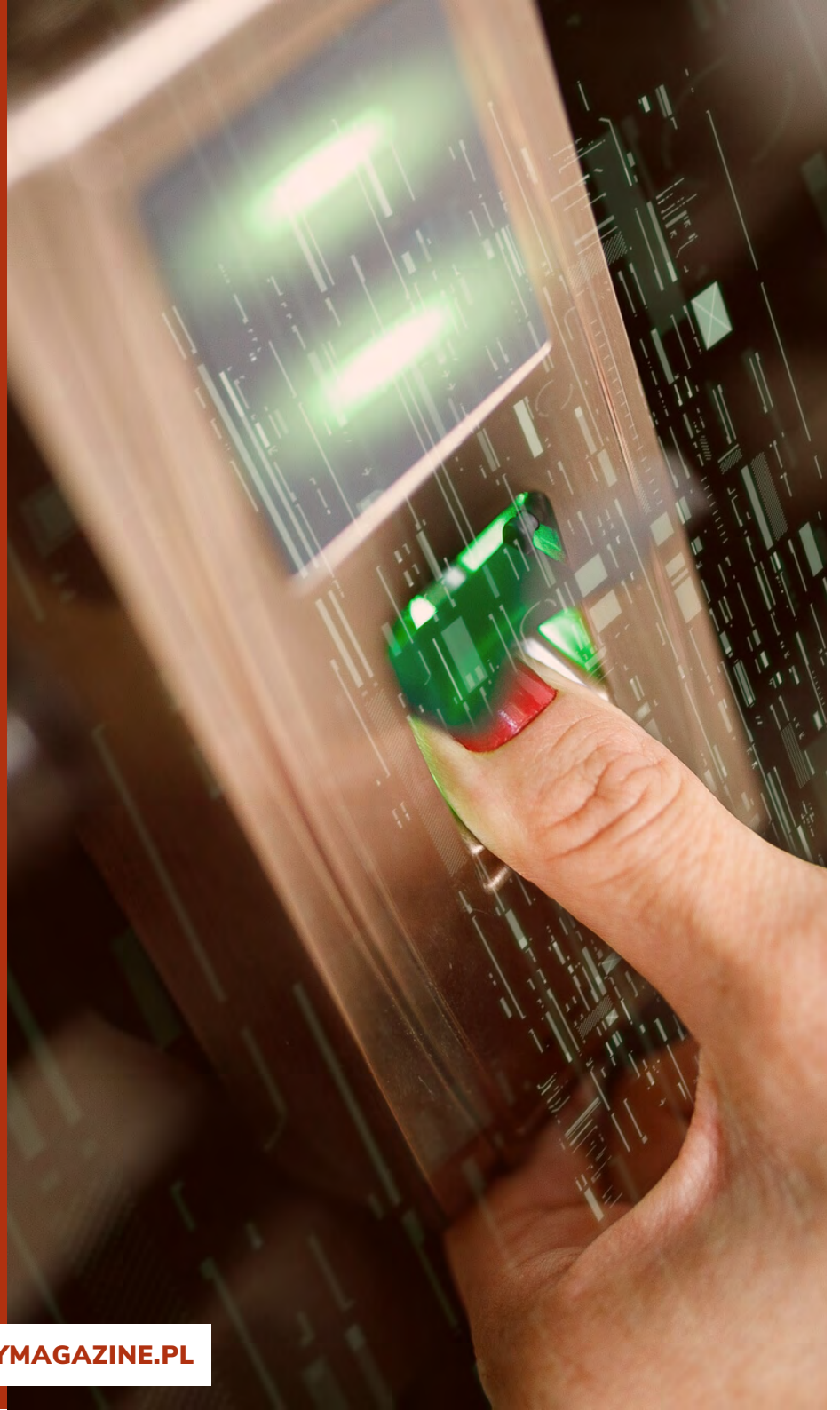
jących na wprowadzeniu bardziej granularnej sieci. Dzięki temu rozwiązaniu hakerzy, zamiast od razu przejść do łamania dostępu do docelowej sieci, muszą jedynie włamać się do dostawcy zarządzania dostępem i wirtualnie osiągnąć to, co mogli przed wprowadzeniem sieci o wysokiej granulacji (ZTA).

Jedyne, co musi zrobić w tym przypadku haker, to wybrać użytkownika lub użytkowników, którzy mają dostęp do docelowych podsieci, a co nie jest trudnym zadaniem przy dzisiejszej globalizacji informacji. Uważaj więc na oferty zarządzania dostępem i upewnij się, że tego właśnie szukasz i że jesteś gotów podjąć to ryzyko.

Przedstawione do tej pory problemy wynikają z braku koncentracji twórców zabezpieczeń na użytkownikach przy rozwiązywaniu problemów związanych z bezpieczeństwem. Założenie, że można wyszkolić ludzi do tego, co należy zrobić, jest nie tylko niewystarczające, ale i rażąco naiwne. Dobre bezpieczeństwo wymaga dobrego systemu, a dobry system musi składać się z dobrych komponentów, które obejmują również użytkowników. Wiemy już, że hasła nie są rozwiązaniem, ale zastąpienie ich urządzeniem, z którym może sobie poradzić każdy, też nie jest właściwym podejściem.

Mamy trzy podstawowe czynniki uwierzytelniania:

1. Co wiesz - np. hasło
2. Co masz - np. urządzenie
3. Czym jesteś – np. pomiary biometryczne.



CO WIESZ

Najtrudniej ukraść to, co jest przechowywane w ludzkim mózgu. Niefortunne jest to, że hasła były nadużywane przez dziesięciolecia i ludzie nie nauczyli się, że nie wolno ich nikomu udostępniać. Ponadto nadmiernie ignorowano ograniczenia ludzkiego mózgu, wymagając zbyt wielu haseł i często żądając zbyt częstej ich zmiany. Zamiast budować system, który jest dla ludzi z ich mocnymi stronami i ograniczeniami, zaczęli prosić jego użytkowników o zrobienie tego, co jest dla nich uciążliwe. Tego rodzaju praktyka jest po prostu nieskuteczna. Wprowadzenie menedżerów haseł tylko pogłębiło problem i teraz przy pojedynczym logowaniu, zwanym podejściem bezhasłowym (SSO), system zdecydował się odrzucić pierwszy czynnik, m.in. co pamiętasz, na korzyść trzeciego czynnika, czyli pomiarów biometrycznych.

Pomiary biometryczne są niebezpieczne dla ich właściciela, ponieważ można je stosunkowo łatwo ukraść, ponadto nie są zbyt wiarygodne i zmieniają się z biegiem czasu, a nawet celowo, jak nowy makijaż, okulary, broda itp. Osoba, której skradziono dane biometryczne (odcisk, próbka głosu itp.) jest zagrożona przez całe życie, po-

nieważ nikt nie może tak po prostu zastąpić skradzionej biometrii inną, tak jak jest to możliwe w przypadku skradzionego, tradycyjnego hasła. Więc znowu uważaj na populizmy, które tak naprawdę nie rozwiązują problemu, są tylko kolejną modą.

CO MASZ

Drugim czynnikiem jest to, co masz, tzn. dowolną namacalną rzeczą, taką jak smartfon, token, sygnet z pieczęcią itp., która jest w posiadaniu danej osoby i którą dana osoba może użyć do identyfikacji. Problem z tym czynnikiem, lub innymi słowy, z rzeczą polega na tym, że może zostać zgubiona, zawieruszona, skradziona, sprzedana, zapomniana lub uszkodzona i być niedostępna w razie potrzeby. Może być również niewłaściwie wykorzystana przez innych do podszywania się pod prawowitego właściciela. Ten czynnik nigdy nie powinien być używany jako główny i jedyny etap uwierzytelniania, ponieważ nigdy nie jest gwarantowane stałe posiadanie konkretnego egzemplarza sprzętu i dlatego nigdy nie powinien on potwierdzać tożsamości użytkownika. Ogólnie rzecz biorąc, im więcej czynników uwierzytelniania zostanie użytych, tym mniejsze szanse na sukces hakera. Chociaż jest to ogólna obserwacja, niezależnie od tego konkretne osoby mogą być całkowicie zagrożone.

Jednym z elementów, który często jest pomijany i może znacząco zwiększyć bezpieczeństwo, jest podzielona wiedza (split knowledge), która choć ma kilka definicji, dotyczy głównie niekompletnych informacji w jednym miejscu w celu odtworzenia lub odszyfrowania danych.

CZYM JESTEŚ

Cała przedstawiona tutaj argumentacja koncentrowała się na prawidłowej weryfikacji tożsamości użytkowników, ponieważ większość naruszeń wynika z wpuszczenia intruza, w oparciu o nieudaną weryfikację tego, kim jest dana osoba. Nie mówię o weryfikacji wszystkich danych osobowych, ale o niezawodnych sposobach, aby upewnić się, że każdego ponownego wejścia dokonuje ta sama osoba, która została w pełni zweryfikowana podczas zakładania konta.

Wielu ma duże nadzieje, że wykorzystując sztuczną inteligencję (AI) będziemy w stanie odpowiednio wcześnie wykryć wtargnięcie do ruchu sieciowego i zmniejszyć lub nawet wyeliminować szkody w przypadku niepowodzenia weryfikacji tożsamości.

Możemy o tym dyskutować, ale trzeba zdać sobie sprawę, że sztuczna inteligencja jest na wczesnym etapie i że „inteligencja" to nic innego, jak mapowanie znanych danych na nieznane funkcje, aby znaleźć kształt tych funkcji w formie numerycznej. Być może uda się znaleźć coś nieznanego, ale ogólnie rzecz biorąc, gdy osoba poufna jest zaangażowana w hakowanie, ruch prawdopodobnie nie różni się od ruchu tworzonego przez legalnego użytkownika, więc wykrycie nie będzie możliwe. Ponadto fałszywe wykrycia mogą stać się dużym utrapieniem dla legalnych użytkowników.

Moim zdaniem, jest to nadal na etapie badań, bardziej praktyczne jest skupienie się na zapobieganiu niż wykrywaniu, mimo że zapobieganie jest znacznie trudniejsze niż wykrywanie.

OCHRONA DOSTĘPU DO AKTYWÓW

Ostatnią rzeczą, o której chciałbym wspomnieć, ale nie najmniej ważną, jest ochrona dostępu do aktywów materialnych, takich jak samochody, domy, biura, transport i wiele innych. Wszystko wokół dostaje swoje komponenty elektroniczne i staje się elektryczne, więc jest bardzo prawdopodobne, że kontrola dostępu wkrótce wykluczy istnienie fizycznych kluczy.

Co to będzie? Karty zbliżeniowe, breloki bezprzewodowe lub jeszcze coś innego? Cóż, to nie jest dobry pomysł, ponieważ im więcej gadżetów każdy musi nosić, tym większe prawdopodobieństwo, że system zawiedzie. Gdy wszystko się łączy, dobre rozwiązanie powinno opierać się na kryptograficznej weryfikacji tożsamości osób.

Chcę tutaj jeszcze podkreślić bardziej niż poprzednio, że czynnik ludzki musi być uwzględniony, ponieważ mówimy o wpuszczaniu osoby fizycznie, a nie tylko cyfrowo, więc szanse na kradzież urządzeń są jeszcze większe, a co za tym idzie, podstawowy czynnik uwierzytelnienia musi skupić się na osobie.

Podsumowując, **krajobraz bezpieczeństwa jest bardzo zdradliwy**, ponieważ chronione systemy nie tylko stają się coraz bardziej złożone, ale także wszechobecne. Teraz nadszedł czas, aby przejść na niezawodne metody identyfikacji użytkowników, oparte na kryptografii i znane nam jako trudne, jeśli nie niemożliwe do złamania. Zegar tyka, a oszuści stają się coraz bardziej przebiegli i lepiej wyposażeni, więc jedynym sposobem na ograniczenie zagrożeń jest wyeliminowanie metod, o których wiemy, że nie działają.

Rozwiązania częściowe nigdy nie będą adekwatne i satysfakcjonujące, zwłaszcza, jeśli istnieją lepsze.

/GDPSYSTEM.EU

ZGODA NA COOKIES

Czy Twoja strona WWW spełnia wymogi prawne i daje możliwość elastycznego zarządzania cookies osobom, które ją odwiedzają?

SPRAWDŹ

SPEŁNIJ WYMOGI PRAWNE

NAJCZĘŚCIEJ WYKRYWANE CYBERZAGROŻENIA W ORGANIZACJACH SŁUŻBY ZDROWIA

Christian Putz
Vectra AI

Dla sektora opieki zdrowotnej, który nie może pozwolić sobie na przerwy w działaniu, cyberataki są bardzo groźne. Vectra AI przeanalizowała najczęstsze zgłoszenia naruszeń wśród klientów z branży zdrowotnej i opracowała raport Spotlight Report-Vision and Visibility: Top 10 Threat Detections Across Microsoft Azure AD and Office 365. Przyjrzyjmy się wnioskom płynącym z tej analizy.

Cyberprzestępcy w swoich działaniach często wykorzystują oprogramowanie ransomware. Ataki tego typu wiążą się z dotkliwymi skutkami finansowymi, wynikającymi z wysokich żądań przestępców w zamian za klucze szyfrujące. Z tego powodu branża ta stanowi częsty cel cyberprzestępców.

Ataki typu ransomware, które są przeprowadzane w instytucjach opieki zdrowotnej, mogą oznaczać kradzież dokumentacji medycznej oraz danych, ale mogą być również fizycznie uciążliwe, powodując opóźnienia w leczeniu pacjentów.

Z tej perspektywy kwestie problemów technicznych stają się mało istotne w porównaniu do problemów, które mogę wpłynąć na stan zdrowia lub zagrozić życiu ludzi. Biorąc pod uwagę fakt, że napastnicy cały czas zdobywają nowe umiejętności i rozszerzają swój zasięg ataku np. na chmurę - w jaki sposób zespoły ds. bezpieczeństwa w opiece zdrowotnej powinny się przygotować by poznając zachowanie i taktykę napastników, skutecznie ich powstrzymać?

Chociaż transformacja cyfrowa poszerzyła obszar ataków, nie oznacza to, że nie można powstrzymać ataków ransomware i innych form

cyberprzestępczości, takich jak przejmowanie kont. Przede wszystkim, trzeba zrozumieć, że ataki ransomware można powstrzymać, ale niekoniecznie można im zapobiec — możemy mieć szansę na uniknięcie kryzysu. Możliwość wykrycia zachowań atakujących już w systemach opieki zdrowotnej jest możliwa dzięki odpowiedniemu monitorowaniu środowiska i widoczności.

NAJCZĘŚCIEJ WYKRYWANE ZAGROŻENIA CYBERNETYCZNE W SŁUŻBIE ZDROWIA

Ostatni raport Spotlight Report-Vision and Visibility: Top 10 Threat Detections Across Microsoft Azure AD and Office 365 szczegółowo analizuje ten scenariusz we wszystkich branżach, jednak poniższe spostrzeżenia koncentrują się na sektorze opieki zdrowotnej. Zawierają najważniejsze zagrożenia zaobserwowane w bazie klientów Vectra AI z sektora zdrowotnego i pokazują, że organizacje opieki zdrowotnej są celem ataków w ramach Microsoft Azure AD i Office 365. Poniższe informacje dotyczące najczęstszych wykryć mogą być wykorzystane, by pomóc w zwiększeniu poziomu bezpieczeństwa pod warunkiem zapewnienia odpowiednich definicji i widoczności.

Potrzebna jest wizja tego, jak powinno wyglądać autoryzowane użytkowanie systemów oraz widoczność pozwalająca monitorować i mierzyć odchylenia od tych definicji.

Chmura ciągle zmienia wszystko, co wiemy o bezpieczeństwie. Tylko odpowiednie wykorzystanie danych przy wsparcie sztucznej inteligencji mogą pomóc w zapewnieniu przejrzystości w chmurze.

Oczywiście należy pamiętać, że wykrycie i reagowanie na zagrożenia są najłatwiejsze, gdy przeciwnicy podejmują działania, które są w oczywisty sposób złośliwe. To sprawia, że niezwykle ważne jest, aby współcześni specjaliści ds. bezpieczeństwa sieci znali punkty wspólne w operacjach, które przeciwnik musiałby podjąć, aby osiągnąć swoje cele, a zachowaniami rutynowo podejmowanymi przez autoryzowanych użytkowników w całym przedsiębiorstwie. Wiele wykryć omówionych w raporcie reprezentuje nietypowe zachowanie i nie wszystkie z nich są spowodowane złośliwą aktywnością.

Zobaczmy, jakie detekcje są często wyzwalane w tym środowisku.

POWER AUTOMATE MOŻE UDOSTĘPNIAĆ DUŻY ZAKRES DOSTĘPU ATAKUJĄCYM

Sektor opieki zdrowotnej zazwyczaj doświadcza ataków na poziomie O365 Suspicious Power Automate Flow Creation, O365 Risky Exchange Operation i O365 Redundant Access Creation.

Najczęstszym wykryciem w sektorze opieki zdrowotnej było O365 Suspicious Power Automate Flow Creation, co może wskazywać, że atakujący konfiguruje mechanizm stałego dostępu. Ten problem odnotował również sektor edukacji (wykrycie w pierwszej trójce), jednak na ogólnej liście 10 najczęstszych wykryć we wszystkich branżach, jest dopiero na siódmym miejscu. Power Automate pomaga zautomatyzować żmudne zadania, takie jak zapisywanie załączników do wiadomości e-mail w usłudze OneDrive, rejestrowanie odpowiedzi na formularze w programie SharePoint i ma wiele innych wygodnych zastosowań. Należy zwrócić uwagę, że jest domyślnie włączony w usłudze Office 365 i standardowo wyposażony w setki łączników.

Najczęściej wykrywane cyberzagrożenia w organizacjach służby zdrowia

Nawet z podstawowym, nieuprzywilejowanym dostępem do Office 365, Power Automate jest potężnym narzędziem, które jest atrakcyjne dla atakujących.

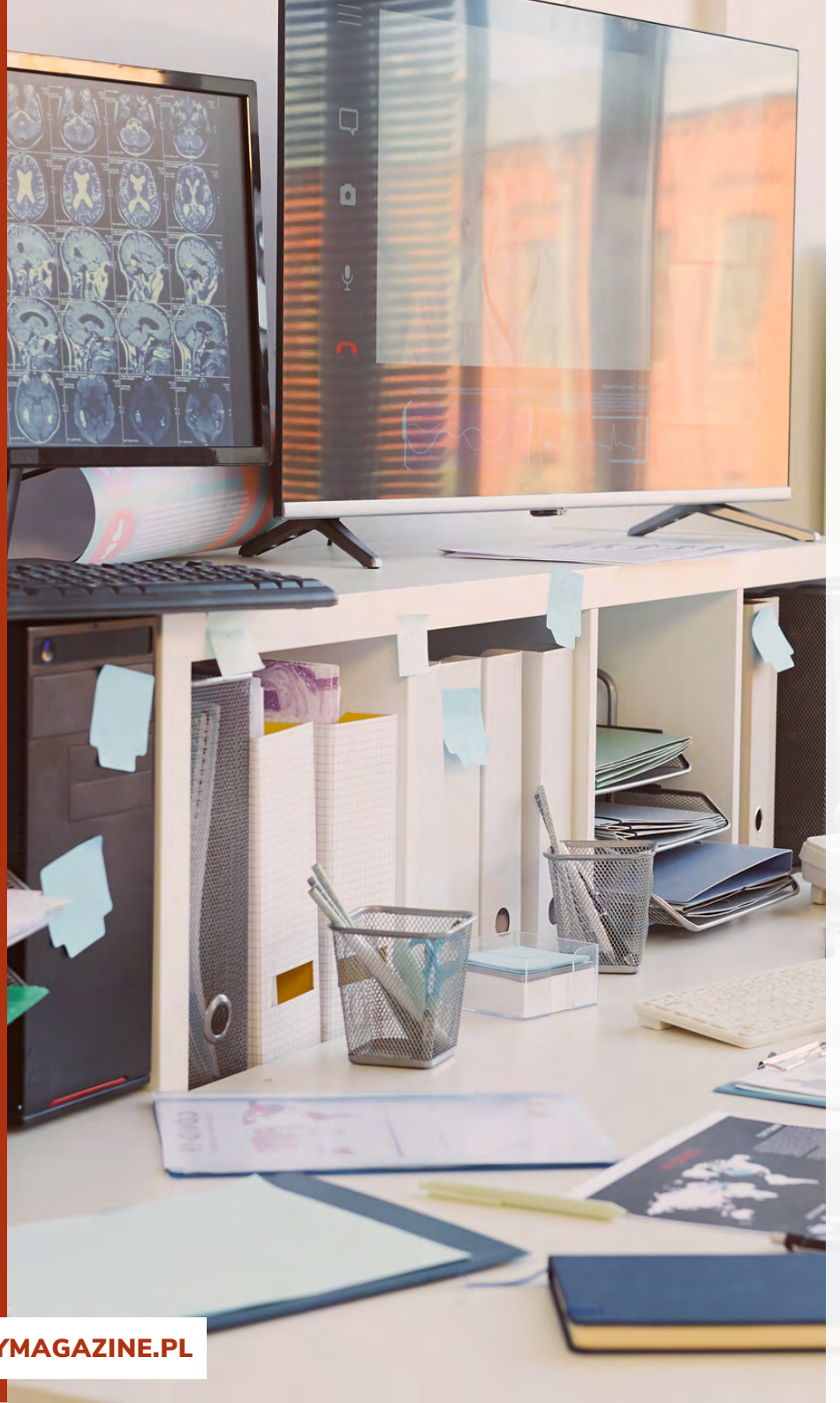
W marcu 2020 roku zespół reagowania Microsoftu odkrył zespół hakerów wykorzystujących Power Automate do eksfiltracji danych w międzynarodowej organizacji, w której napastnicy pozostali niewykryci przez 213 dni. Wynika z tego, że wszystkie międzynarodowe organizacje powinny zracjonalizować dostęp do Power Automate Flow tylko dla użytkowników, którzy tego dostępu wymagają i ściśle monitorować manipulacje kontami, które mogą prowadzić do zwiększenia uprawnień i kradzieży informacji.

Oprócz wykrycia O365 Suspicious Power Automate Flow Creation, klienci z sektora opieki zdrowotnej doświadczyli również wykrycia O365 Risky Exchange Operation i O365 Redundant Access Creation, które znalazły się w pierwszej trójce. Wykrycie O365 Risky Exchange Operation może wskazywać, że zapewniony jest dostęp do wrażliwych informacji, które byłyby dostępne w poczcie elektronicznej, co może wskazywać, że atakujący manipuluje serwerami Exchange w celu uzyskania dostępu do danych, umożliwiających dalszą penetrację systemów. Natomiast O365 Redundant Access Creation oznacza, że uprawnienia administracyjne zostały przypisane do nowego podmiotu, co może z kolei może wskazywać, że atakujący zapewnia sobie namiarowe dostępy by poradzić sobie z reakcją zespołu bezpieczeństwa.

Ogólnie rzecz biorąc, klienci z sektora opieki zdrowotnej wykazywali niższą względną częstotliwość wykrywania w porównaniu z większością innych branż. Jednak automatyzacja przepływów pracy za pomocą Power Automate i nadawanie praw administracyjnych aplikacji, użytkownikowi lub zleceniodawcy usługi to usługi, które napastnicy często wykorzystywali do uzyskania dostępu do poczty elektronicznej i poufnych informacji. Są obecne w Office 365, z którego korzystają wszyscy klienci, co sprawia, że pełna widoczność aktywności kont jest kluczową częścią zarządzania bezpieczeństwem.

ZNAJOMOŚĆ ZACHOWAŃ "TWOJEGO" KONTA

Niezależnie od branży, atakujący chętnie wybierają chmurę jako cel ataków. Office 365 to niezwykle użyteczne i potężne narzędzie – dlatego za dostęp do niego płaci ponad 250 milionów osób. Tak duża aktywność użytkowników jest postrzegana przez atakujących jako ogromna szansa, nic dziwnego, że wykazują motywację do obrania za cel każdej organizacji, w której istnieje możliwość wyłudzenia pieniędzy lub kradzieży aktywów.



Microsoft Office 365 i Azure AD to tylko część dużej powierzchni ataku, którą organizacje muszą zarządzać, ale jak wykazano na przykładzie Power Automate, które jest niezwykle wygodne dla automatyzacji i przyspieszania procesów, otwiera wiele możliwości hakerom. Dlatego niezwykle ważne jest, aby zrozumieć ryzyko i dokładnie wiedzieć, jak używane są takie narzędzia.

Różnica między zachowaniem napastników i prawidłowych uprzywilejowanych kont może być bardzo rozmyta bez możliwości zbierania właściwych danych, które są odpowiednio dopasowane do definicji zachowań i widoczności. Ważne jest, aby dojść do punktu, w którym wiadomo, jak wygląda autoryzowane użycie, aby zrozumieć zachowania, które podejmują przeciwnicy. Odpowiednio wyposażona SI może pomóc zamknąć luki bezpieczeństwa w Office 365 i Azure AD, udostępniając dane i sygnalizując, gdy dzieje się coś niestandardowego.

Cyber 24 DAY

12 października 2022

Warszawa, Hotel Sofitel Warsaw Victoria

Army

Cyber

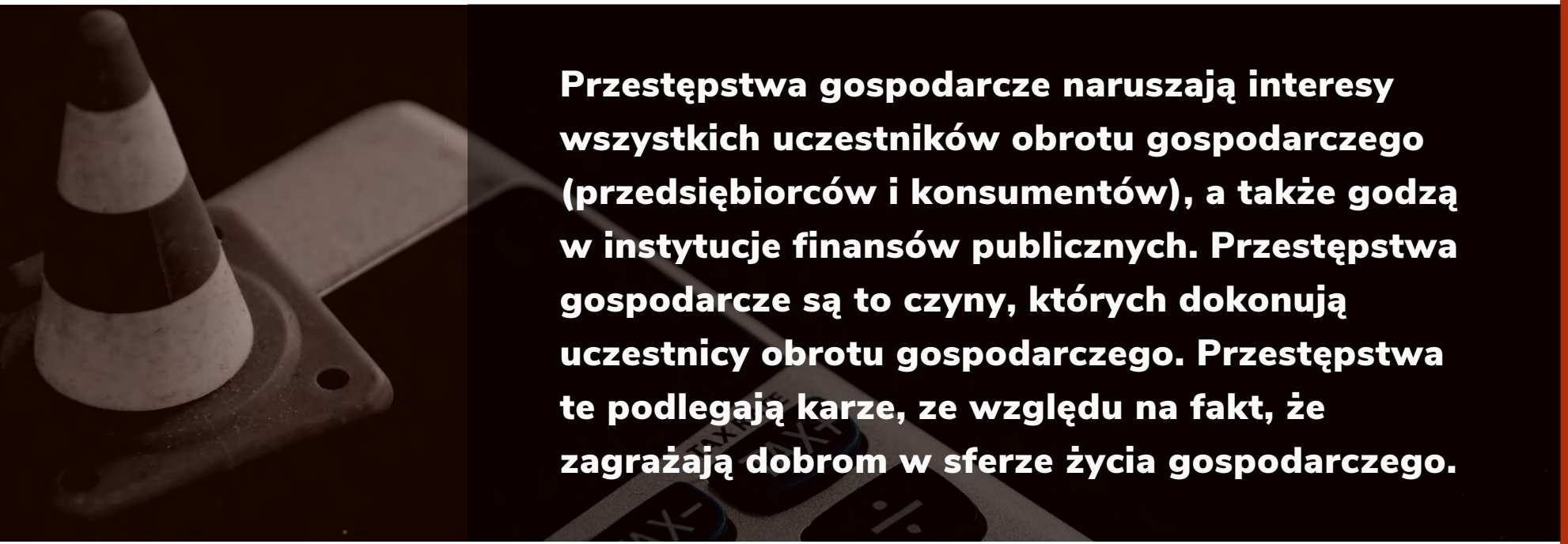
Public&Policy

Tech

#Cyber24Day

PRZESTĘPCZOŚĆ GOSPODARCZA JAKO ZAGROŻENIE STABILNOŚCI FIRMY

insp. dr Mariusz Ciarka
Komenda Główna Policji



Przestępstwa gospodarcze naruszają interesy wszystkich uczestników obrotu gospodarczego (przedsiębiorców i konsumentów), a także godzą w instytucje finansów publicznych. Przestępstwa gospodarcze są to czyny, których dokonują uczestnicy obrotu gospodarczego. Przestępstwa te podlegają karze, ze względu na fakt, że zagrażają dobrom w sferze życia gospodarczego.

CZYM JEST PRZESTĘPSTWO GOSPODARCZE?

W polskim porządku prawnym nie funkcjonuje legalna definicja przestępstwa gospodarczego. Literatura prawnicza i ekonomiczna określa przestępstwo gospodarcze jako czyn zabroniony, godzący lub zagrażający ponadindywidualnym dobrom w sferze życia gospodarczego, polegający na naruszeniu zaufania związanego z pozycją sprawcy lub instytucją życia gospodarczego, grożący utratą zaufania do systemu gospodarczego lub jego podstawowych instytucji.

Mając na uwadze fakt, iż gospodarka jest tą dziedziną życia, która służy pomnażaniu dóbr o charakterze majątkowym, korzyść majątkowa była i jest nieodłącznym elementem aktywności gospodarczej. Ta sfera stosunków społecznych jest szczególnie narażona na niebezpieczeństwo zachowań sprzecznych z prawem i wartościami, na których opiera się ład społeczny.

Za cechy przestępczości gospodarczej dostrzegane we wszystkich jej koncepcjach uznaje się zwłaszcza:

- brak w działaniach sprawców przemocy, która zastępowana jest działaniami mającymi pozory legalności, a polegającymi najczęściej na nadużywaniu instytucji życia gospodarczego, funkcjonujących w znacznym stopniu na zasadach publicznego zaufania,
- poważne straty materialne i niematerialne jako następstwa takich działań, przy czym te ostatnie wykraczają niekiedy poza sferę życia gospodarczego (np. w przypadku korupcji),

- fakt, że ofiarami są głównie anonimowe osoby, gałęzie i instytucje systemu gospodarczego,
- stosunkowo znaczna liczba sprawców rekrutuje się z wyższych warstw społecznych.

NA ZAKWALIFIKOWANIE DANEGO ZDARZENIA TJ. CZYNU ZABRONIONEGO SPOŁECZNIE SZKODLIWEGO, JAKO „PRZESTĘPSTWA GOSPODARCZEGO” DECYDUJE DE FACTO PRAKTYKA ORGANÓW ŚCIGANIA (POLICJI, PROKURATURY). ORGANY, USTALAJĄC WŁAŚCIWOŚĆ MERYTORYCZNĄ SWOICH KOMÓREK ORGANIZACYJNYCH, OKREŚLAJĄ WYMIENIONĄ PRZESTĘPCZOŚĆ.

Wyrazem powyższego mogą być wydziały w powszechnych jednostkach organizacyjnych prokuratury, którym przypisywana jest właściwość merytoryczna prowadzenia lub nadzorowania postępowań przygotowawczych tradycyjnie określanych jako przestępstwa gospodarcze. W zależności od szczebla danej jednostki mogą to być wydziały postępowań przygotowawczych, wydziały śledcze, wydziały do spraw przestępczości zorganizowanej.

W jednostkach Policji na szczeblach wojewódzkich utworzono natomiast Wydziały do walki z Przestępczością Gospodarczą. Jednym z kluczowych zadań Wydziałów do walki z Przestępczością Gospodarczą jest zbieranie informacji w aspekcie pracy operacyjnej oraz prowadzenie postępowań przygotowawczych dotyczących naruszenia przepisów o charakterze gospodarczym zawartych w ponad stu aktach prawnych, w których wpisane do systemu kar są rzeczone przestępstwa.

Przykładowo można tu wskazać przestępstwa:

- polegające na fałszowaniu dokumentów i używanie ich jako autentycznych oraz poświadczenia nieprawdy w dokumentach,
- przeciwko mieniu, czyli wszelkiego rodzaju przywłaszczenia wyłudzenia pieniędzy i towarów,
- przeciwko obrotowi gospodarczemu, tj. wyłudzenia kredytów, pożyczek bankowych, wyłudzenia odszkodowań z tytułu umowy ubezpieczenia, pranie brudnych pieniędzy, udaremnienie egzekucji komorniczej, nierzetelne prowadzenie dokumentacji działalności gospodarczej i udaremnienie przetargów publicznych,

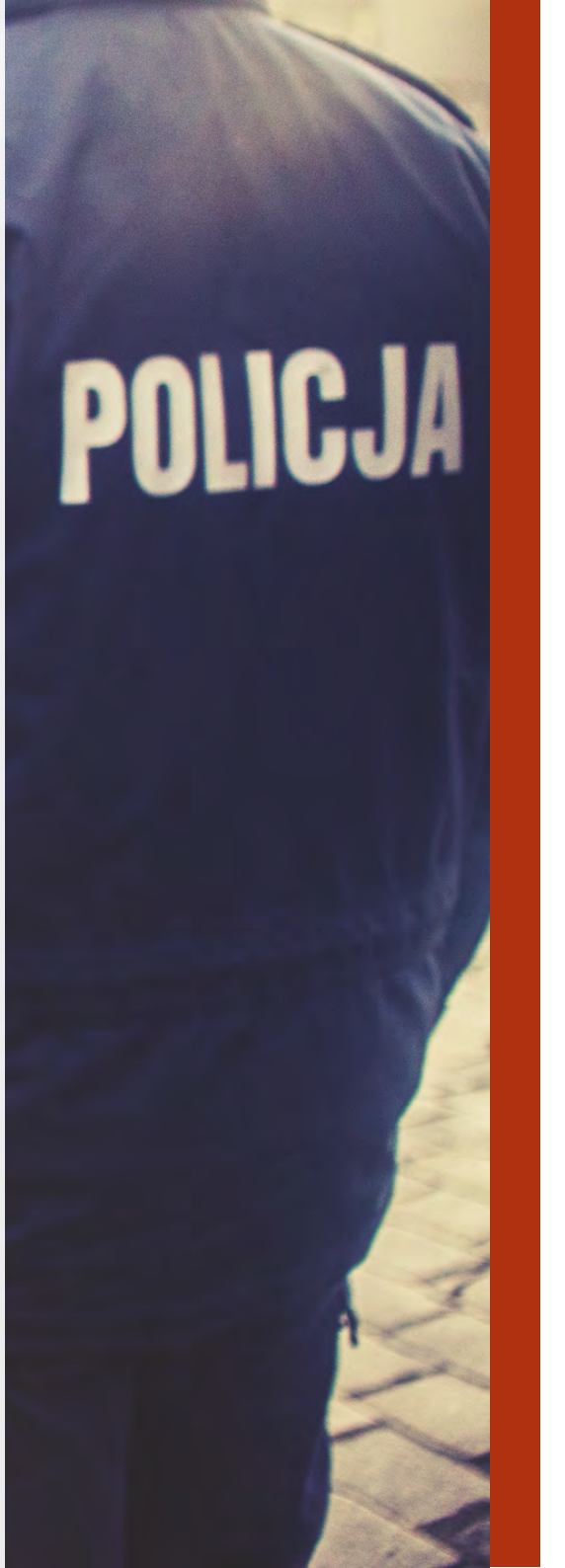
- dotyczące uzyskania cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej – oszustwa internetowe,
- intelektualne, w tym wprowadzenia do obrotu towarów oznaczonych podrobionym znakiem towarowym,
- dotyczące sprzedaży napojów alkoholowych bez wymaganego zezwolenia, rozlewu wyrobów spirytusowych oraz wytwarzania wyrobów tytoniowych bez wymaganego zezwolenia,
- przestępczość paliwowa,
- przeciwko środowisku (negatywne następstwa działalności gospodarczych),
- przeciwko prawom pracowniczym (łamanie praw pracownika w zakładach pracy).

Podziałowi na kilka grup podlegają sprawcy przestępstw gospodarczych. Wyróżnia się wśród nich sprawców:

- zawodowych
- sytuacyjnych
- okazjonalnych.

W okresie styczeń - sierpień 2022 roku w Polsce stwierdzono 173.603 przestępstw gospodarczych. Wykrywalność przestępstw gospodarczych w tym czasie wyniosła 77,99 procent.

Zawiadomienie o popełnieniu przestępstwa, również gospodarczego, można złożyć na dwa sposoby. Osobiście we właściwej jednostce Policji, czyli obejmującym swoim zasięgiem działania miejsce czynu, albo pisemnie wysyłając stosowny dokument do Policji czy Prokuratury.



W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

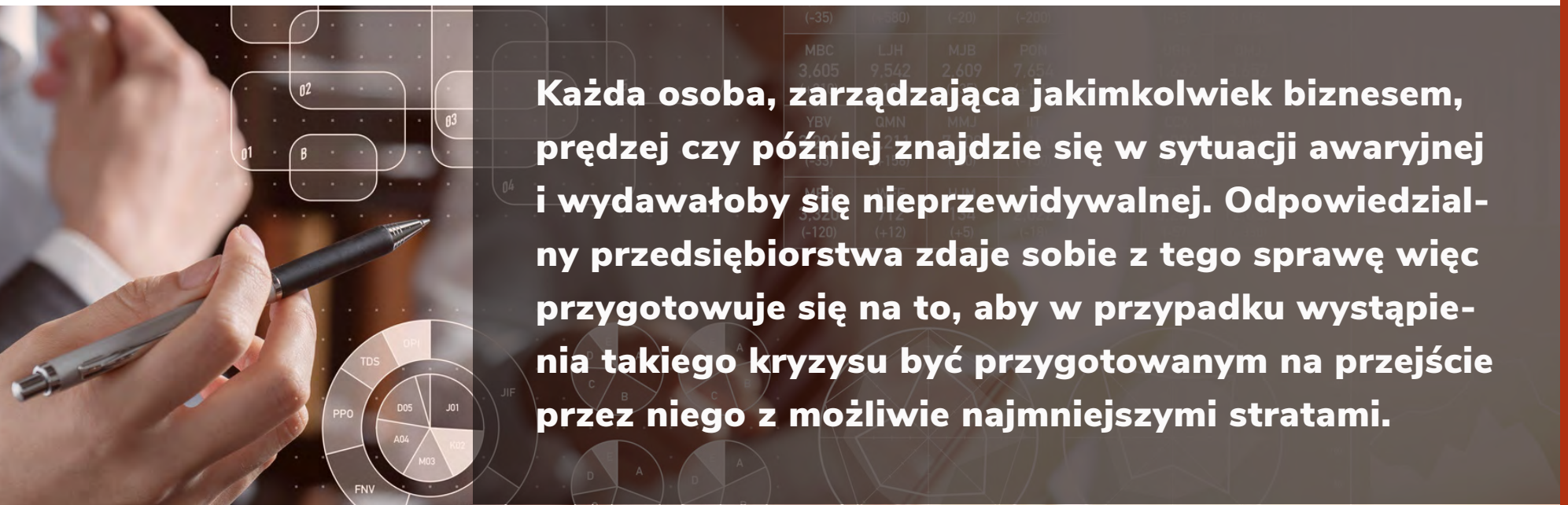
MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

WYWIAD I KONTRWYWIAD BIZNESOWY W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA W FIRMIE

Maciej Zygmunt
Agencja Bezpieczeństwa i Detektywistyki



Każda osoba, zarządzająca jakimkolwiek biznesem, prędzej czy później znajdzie się w sytuacji awaryjnej i wydawałoby się nieprzewidywalnej. Odpowiedzialny przedsiębiorstwa zdaje sobie z tego sprawę więc przygotowuje się na to, aby w przypadku wystąpienia takiego kryzysu być przygotowanym na przejście przez niego z możliwie najmniejszymi stratami.

ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

Za płynne przechodzenie przez sytuacje kryzysowe jest odpowiedzialna właśnie ta część działalności zarządczej, którą nazywamy „zarządzaniem ciągłością działania". Jej zadaniem jest opracowanie takich planów, które krok po kroku przeprowadzą organizację przez wszystkie możliwe zagrożenia. Wszystkie te kroki powinny być rozpisane na role, czyli, krótko mówiąc, poszczególne zadania z takiego planu powinny być przypisane konkretnym osobom odpowiedzialnym za ich realizację.

Oczywiście, wiele podmiotów posiada różnego rodzaju, wewnętrzne regulaminy przewidujące, kto i jak powinien zachować się w przypadku zaistnienia określonych sytuacji. Jednak moje wieloletnie doświadczenia w działaniach związanych z bezpieczeństwem biznesu pozwalają na to, że bez obawy o błędną diagnozę, mogę powiedzieć, że w zdecydowanej większości firm, prawidłowe zarządzanie ciągłością działania nie istnieje, a podmioty te zwracają się o pomoc do takich firm, jak Agencja Bezpieczeństwa i Detektywistyki dopiero, gdy kryzys nie tylko wystąpił, ale poczynił już w firmie wymierne straty.

Zawsze cieszę się, gdy podejmowane w sytuacjach kryzysowych działania, skutkują stworzeniem w firmie procedur, które mają zapobiec podobnym przypadkom w przyszłości oraz planem postępowania, na wypadek, gdy jednak do nich dojdzie.

Największą satysfakcję zawodową odczuwam jednak wtedy, gdy przedsiębiorca decyduje się na rozwiązanie najlepsze, a najlepszym rozwiązaniem jest właśnie prawidłowe zarządzanie ciągłością działania, a nie ograniczanie się do gaszenia pożarów.

Jak już wspomniałem, prawidłowa realizacja działań zarządczych w tym zakresie to przygotowanie odpowiednich scenariuszy na wypadek wystąpienia zagrożenia, najlepiej takich, które do wystąpienia sytuacji kryzysowej nie dopuszczą, ale gdy jednak już taka się zdarzy, pozwolą na sprawne zarządzanie firmą, pozwalające skutki kryzysu zminimalizować.

Bazą do przygotowania takich planów powinna być prawidłowa analiza zagrożeń. I tutaj dochodzimy do tytułowej, roli wywiadu i kontrwywiadu biznesowego, dzięki któremu, jesteśmy w stanie możliwe zagrożenia prawidłowo zdiagnozować.

Bo oczywiste jest, że aby poddać analizie jakieś dane wyjściowe, musimy te dane, czyli odpowiednie informacje posiadać. Do tego zaś nieodzowny jest wywiad i kontrwywiad biznesowy. Właśnie wywiad biznesowy ma wspierać decyzje przedsiębiorców przez pozyskiwanie, analizowanie i przetwarzanie informacji wywiadowczych, które następnie są wykorzystywane w działaniach lub tworzone są z nich rekomendacje dla zarządu przedsiębiorstw, a jedną z najważniejszych sfer działania takiego wywiadu jest pozyskiwanie informacji i analiza tego, co nazywamy otoczeniem makroekonomicznym danego przedsiębiorstwa, a więc nie tylko firmy konkurencyjne, ale także dostawcy i klienci.

Najlepiej jednak, gdy analiza ta bada także wszystkie inne zjawiska i zdarzenia zachodzące wokół firmy oraz obejmuje ich wpływ na przedsiębiorstwo.

Tu myślę np. o takich zdarzeniach, które bezpośrednio nie są zależne od człowieka. Przykłady: zmiany klimatyczne, polityczne czy epidemie, których wystąpienie, o czym dzisiaj nie muszę już chyba przekonywać, jest w stanie przewrócić do góry nogami gospodarkę, poprzez zmiany priorytetów rynkowych lub np. przerwanie dotychczasowych łańcuchów dostaw albo zablokowanie rynków zbytu.

Przynajmniej część z osób czytających ten tekst zgodzi się teraz z tym, że wywiad biznesowy może być (moim zdaniem powinien być) ważnym składnikiem zarządzania.

CO Z KONTRWYWIADEM?

Co on ma wspólnego z zarządzaniem przedsiębiorstwem, nawet w tej części, którą określamy zarządzaniem ciągłością działania? Przecież w popularnej, encyklopedii internetowej przeczytamy, że: „*W Polsce kontrwywiadem cywilnym zajmuje się Agencja Bezpieczeństwa Wewnętrznego, a wojskowym Służba Kontrwywiadu Wojskowego, która zajmuje się też kontrwywiadem radioelektronicznym.*”

Więc gdzie tu miejsce na zarządzanie ciągłością działania w przedsiębiorstwie? Odpowiem przykładem sprawy, którą ostatnio się zajmowałem. Zarząd dużej firmy powierzył stanowisko dyrektora jednego z jej oddziałów, wydawało się osobie idealnej do tego, aby jak to się nieraz mówi „zrobić porządek w firmie”. Oparto się na tym, że osoba ta miała cechy świetnego przywódcy, który potrafi wymusić posłuszeństwo i podejmować szybkie decyzje. Jej atutem miało być też to, że dobrze znała specyfikę firmy, gdyż wcześniej zajmowała się w niej sprzedażą.

Po trzech latach sprawowania przez tą osobę funkcji dyrektora okazało się, że Oddział którym kierowała nie tylko przynosi wielomilionowe straty, ale pociągnął za sobą całą spółkę, która stanęła na skraju bankructwa i dzisiaj nadal nie wiadomo, czy się z tego podniesie. Długo tłumaczono to sobie tzw. siłą wyższą to znaczy utratą rynków spowodowaną pandemią COVID.

Co ciekawe, do mnie zwrócono się o pomoc w wyjaśnieniu podejrzenia sabotażu, w wyniku którego firma poniosła orgomne koszty związane z reklamacją dużej partii ich produktów, a w konsekwencji groźbą utraty jednego z kluczowych odbiorców.

Czynności w tej sprawie ujawniły właśnie sposób zarządzania oddziałem przez jego dyrektora, który doprowadził do tragicznej sytuacji całej firmy. Okazało się, że osoba ta, wcześniej doskonale radząca sobie w sprzedaży, nie miała żadnych kompetencji do zarządzania sprawami związanymi z zaopatrzeniem i produkcją, i podejmowała decyzje w wyniku których, kupowano na przykład części zupełnie nie nadające się do wykorzystania w produkcji tej firmy ze względu na ich niską jakość, a nawet dlatego, że takie części w tej produkcji nie miały zastosowania.

Mało tego, w trakcie prowadzonych czynności okazało się, że dyrektor od kilku miesięcy jest umówiony na przejście do konkurencyjnej wobec mojego zleceniodawcy firmy, a mając to na uwadze podjął szereg czynności, które wyczerpują znamiona przestępstw zarówno z ustawy o zwalczaniu nieuczciwej konkurencji, jak i kodeksu karnego, przekazując mu m.in. kontakty do kontrahentów, jak i inne informacje stanowiące tajemnicę przedsiębiorstwa.

Przykład powyższy obrazuje idealnie tezę, że kontrwywiad biznesowy jest bardzo ważny jeśli przedsiębiorca poważnie myśli o tym, aby unikać sytuacji kryzysowej. W powyższym przypadku brak takich działań doprowadził firmę do sytuacji olbrzymiego kryzysu, z którego nawet jeśli uda się wyjść, to będzie to okupione olbrzymimi stratami, zarówno finansowymi, jak i wizerunkowymi.

Można było tego uniknąć, bo to do zadań kontrwywiadu biznesowego należy m.in.:

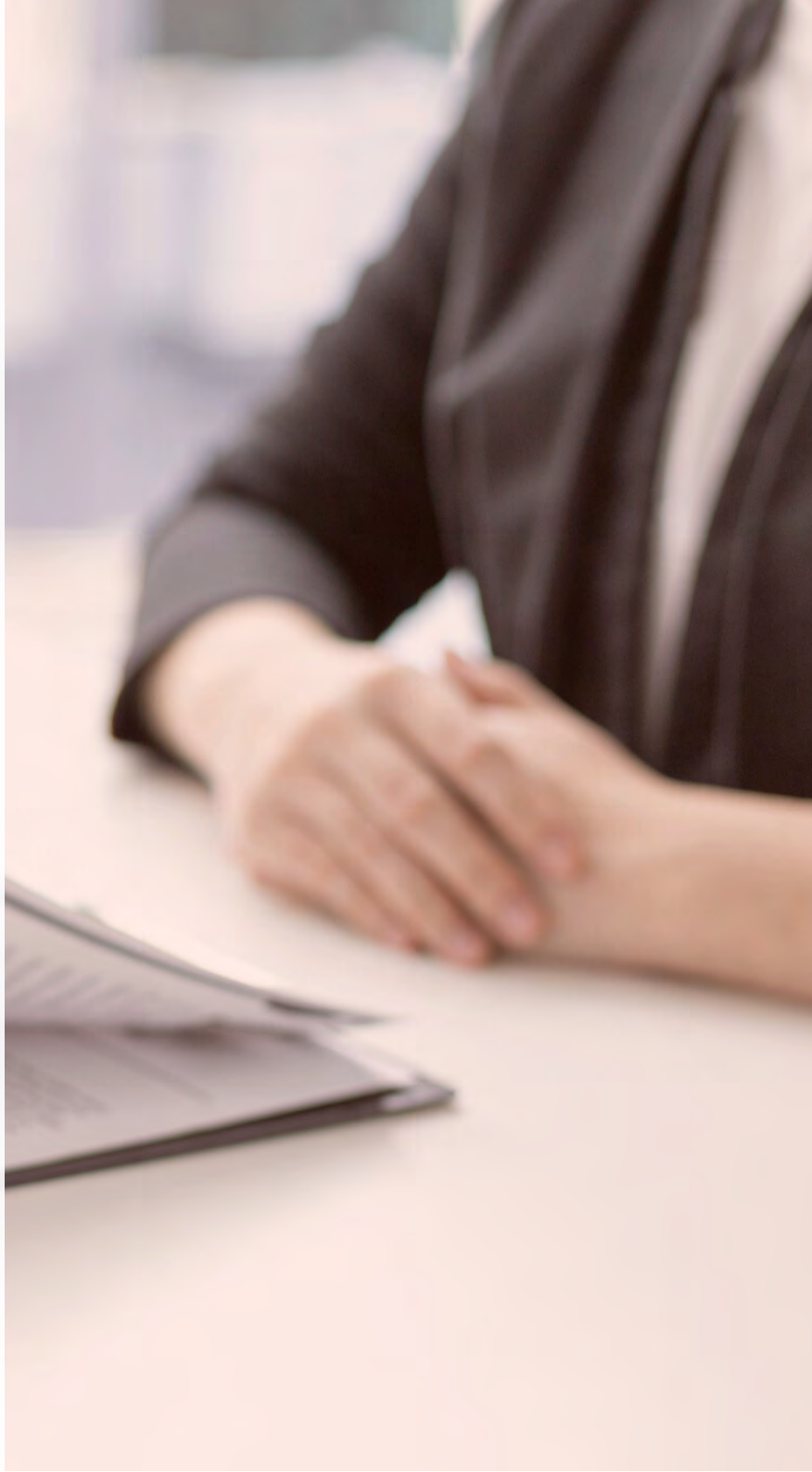
- **monitoring środowiska wewnętrznego** - pozyskiwanie informacji związanych z lojalnością pracowników czy przestrzegania standardów przez kadrę kierowniczą i osoby funkcyjne;
- **weryfikacja dostępu podmiotów zewnętrznych** do informacji o przedsiębiorstwie, członkach zarządu, kadrze kierowniczej;
- **przeciwdziałanie szpiegostwu** przemysłowemu i czynom nieuczciwej konkurencji.

Ważnym zadaniem kontrwywiadowczym jest także tzw. **monitoring medialny środowiska zewnętrznego** danej organizacji/przedsiębiorstwa, aby w odpowiednim czasie i adekwatny sposób reagować na zdarzenia, które mogą mieć znaczenie dla niego znaczenie.

Podsumowując związki wywiadu i kontrwywiadu biznesowego z zarządzaniem ciągłością działania można powiedzieć, że nie ma takiego zarządzania bez dostępu do informacji, które zapewnić może tylko profesjonalna działalność wywiadowcza, a następnie solidna analiza tych informacji.

Oczywiście, sama skala działań wywiadu i kontrwywiadu biznesowego powinna być dostosowana do specyfiki i wielkości przedsiębiorstwa, którego dotyczy. Nawet jednak takie firmy, które niekoniecznie muszą mieć swoje komórki zajmujące się pozyskiwaniem i analizą informacji, powinny korzystać w znacznie większym zakresie niż to dzieje się w Polsce, przynajmniej z profesjonalnego doradztwa w tym zakresie oraz współpracować z zewnętrznymi podmiotami wyspecjalizowanymi w takiej działalności.

Śmiem zresztą twierdzić, że znaczna część podmiotów zostanie do korzystania z takiego narzędzia jak wywiad i kontrwywiad gospodarczy pośrednio zmuszona przez zmiany prawne. Myślę tu głównie o zapowiadanych zmianach w ustawie o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary oraz o wejściu w życie ustawy wprowadzającej do polskiego prawa rozwiązania prawne wynikające z Dyrektywy UE i PE o ochronie sygnalistów. To już jednak temat na kolejny artykuł.



ABD

Agencja Bezpieczeństwa i Detektywistyki

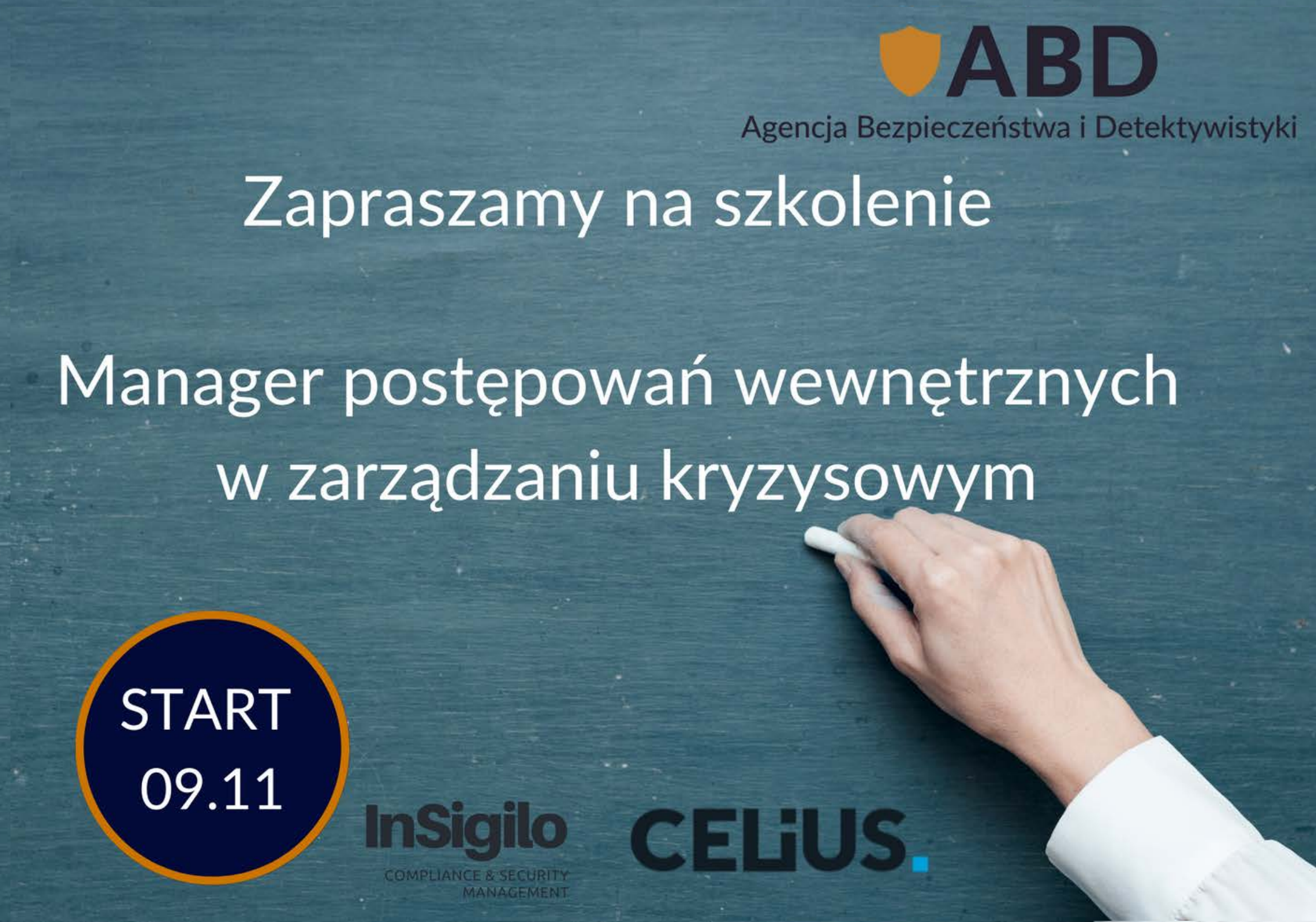
Zapraszamy na szkolenie

Manager postępowań wewnętrznych w zarządzaniu kryzysowym

START
09.11

InSigilo
COMPLIANCE & SECURITY MANAGEMENT

CELiUS.



ZAKUPY W ONLINE BEZ OSZUSTW

Joanna Gizgier
byfehu.art

Dynamiczność z jaką rozwija się świat IT możemy obserwować już od dawna, jednak niewielu ma tego absolutną świadomość.
Czy samodzielnie dokonujesz analiz, w jaki sposób jesteś kierowany, kierowana przez UX-owy design e-sklepu? W ilu krokach jesteś w stanie dokonać bezpiecznego e-zakupu i dlaczego?

BĘDĄC PRZEDSIĘBIORCĄ JESTEŚ TEŻ KLIENTEM

Cyfryzacja przedsiębiorczości osiąga stan rewolucyjny w chwili obecnej. Wchodzimy w internet 5G, digitalizacja jest podstawą każdej firmy chcącej mieć znaczenie na rynku. Innowacyjność Polski nadała kierunek wiodącej i znaczącej pozycji w światowej branży ewolucji współczesnych firm. Pominę już wprowadzenie, co było kiedyś podczas zakupów internetowych. Teraz jest teraz. Wszystko się zmieniło z dnia na dzień i czasy raczkującego i nieumiejętnego handlu elektronicznego minęły bezpowrotnie.

Jesteś przedsiębiorcą i klientem jednocześnie, więc wiesz, że kierujesz się wygodą połączoną z bezpieczeństwem, a jednocześnie skłania Cię do wyborów przekaz korzyści, jakie napłyną do Ciebie. Przestańmy się oszukiwać, że wystarczy nam zainstalowany przez **autoinstalator WordPress** z darmowym lub płatnym szablonem i podmienienie w nim zdjęć i treści do podbicia rynku swoją firmą, po czym będziemy próbować zlecić pozycjonowanie jakiejś kolejnej firmie, łudząc się, że przyniesie nam to sprzedaż.

CO POWINNO WZBUDZIĆ NASZ NIEPOKÓJ?

Pierwszy alarm to brak www, to najszybsze źródło oszustw. Pamiętaj, nie ma nic za darmo. Jeżeli widzisz bardzo zaniżoną cenę, czy to w portalu społecznościowym czy sklepie on-line, zastanów się dwa razy, co jest powodem tak dużej obniżki. Lubimy okazje, bardzo często dajemy się złapać na "ofertę ważną tylko przez godzinę" lub tanio i profesjonalnie, ostatnie sztuki jakiegoś produktu itp. Kupujemy oczami, więc często bardzo atrakcyjne zdjęcie może całkowicie wyłączyć nasze krytyczne myślenie i nie zauważymy, że za niską cenę kupiliśmy "zdjęcie samochodu" albo mini wersję stołu który w rzeczywistości nadaje się nie do salonu tylko do domku lalek, tak były takie aukcje na popularnych w Polsce czy w Chinach portalach.

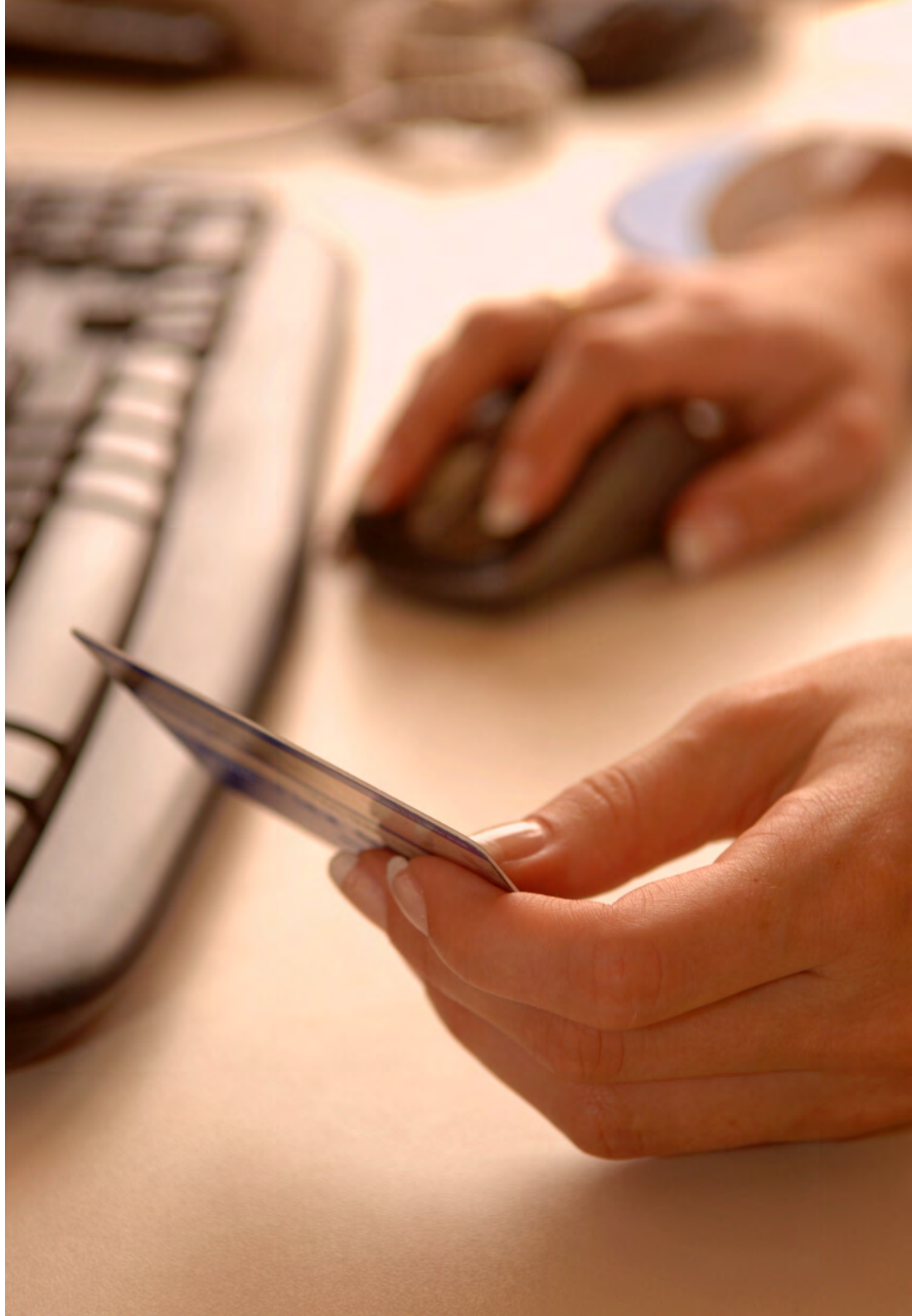
Kolejnym dzwonkiem alarmowym może, być oferta wysłana w pięć minut, napisana w taki lakoniczny sposób, aby pozostawić przestrzeń na niedomówienia, z których później łatwo się będzie wytłumaczyć. Bo przecież sukienka ze zdjęcia wygląda prawie tak samo, jak ta na żywo, nie ukryto jej stanu, a że zdjęcie było niewyraźne, to już przecież nie wina autora ogłoszenia.

Oczywiście, złe opinie o sklepie, brak kontaktu do sprzedawcy czy procedur zwrotu czy reklamacji na stronie też mogą, chociaż nie muszą, świadczyć o pewnych ryzykach.

JAK BYĆ BEZPIECZNYM W CZASIE E-ZAKUPÓW?

Podczas zakupów za pośrednictwem serwisów aukcyjnych czy w e-sklepach warto sprawdzić czy sprzedawca jest przedsiębiorcą. Kupujący podlega ochronie prawnej przewidzianej dla konsumentów tylko w przypadku gdy zawiera umowę z przedsiębiorcą. Możemy to zrobić, wpisując NIP lub nazwę i adres sprzedawcy na stronach: CEDIG czy EMS

Prostym narzędziem jest też weryfikacja oferty na stronach Google i tu autentyczność, jawność musi rzucać się w oczy.



Nie bez znaczenia ma też jakie wrażenie wywrze na Tobie dobrze działająca strona www, która jest znacząca i na rynku i dla algorytmów oraz nie ma negatywnych opinii. To jest wyczyn pracochłonny i absolutnie świadomie wyczynem wypracowanym, więc trudno jest posiadać taką stronę czy fanpage gdy firma zakłada szybką akcję nakierowana tylko na nielegalny zysk i oszustwo. Zbyt duża inwestycja, obarczona zbyt dużym ryzykiem.

Wiele oszust odbywało się też często wtedy gdy klienci nie mogli polegać na płatnościach wspieranych przez systemy finansowe, takie jak bramki płatnicze, wirtualne portfele czy bezpieczne płatności kartą. Podawanie numeru karty mailem, płatność przelewem na podstawie maila, czy np. w przypadku aukcji, pomijanie w korespondencji przez platformy sprzedażowe, często kończą się utratą środków lub, co możemy uznać za szczęście, nerwami.

NA CO WIĘC ZWRACAĆ NAJWIĘKSZĄ UWAGĘ?

Zasad jest kilka, nie różnią się one tak naprawdę bardzo od tych, którymi kierujemy się w rzeczywistym świecie. Pomyśl, że kupujesz coś dość drogiego, powiedzmy komputer.

JAKIE KRYTERIA BĘDZIESZ BRAĆ POD UWAGĘ, SZUKAJĄC SKLEPU W REALNYM ŚWIECIE?

Profesjonalny i godny zaufania sprzedawca. Wielkość sklepu, oczywiście nie musi to być wielki market elektroniczny, w wielu wypadkach mniejsza firma z bardziej indywidualnym podejściem, może mieć lepszą doradczość. Ważne, żeby zweryfikować jej opinie oraz historię i legalność działania.

Ceny zbliżone do rynkowych. Możesz zweryfikować je na portalach takich jak Ceneo itp., Zbyt niska cena, nierealna lub bardzo odbiegająca od średniej to często oszustwo.

Brak regulaminów sprzedaży i zwrotów, ale też zbyt rozbudowane i skomplikowane lub mające wiele błędów, to też powód do obawy. W dzisiejszych czasach powinniśmy również zwracać uwagę na politykę prywatności i zapisy związane z RODO.

Niektóre strony mogą nie oszukać nas na zakupie, ale **będą zbierały dane,** które potem mogą być wykorzystane do celów handlowych czy cyberataków.

Brak wspieranych systemów płatności online. Jeżeli jedyne, co możesz zrobić, to wysłać przelew przed złożeniem zamówienia, a do tego zamówienie nie jest wspierane przez żaden system pozostawiający ślad zamówienia po Twojej stronie, lepiej w takiej sytuacji z niego zrezygnuj.

Nie każda rekomendacja jest równa. Nawet jeżeli na Facebooku firmy widzisz tysiące obserwujących, popatrz ile reakcji widzisz pod poszczególnymi postami. Popularnym, chociaż bardzo nieetycznym jest "kupowanie" followersów. Takie puste konta jednak nie "lajkują" i nie komentują. Więc jeżeli portal ma kilkanaście tysięcy lubiących obserwujących, a brak zaangażowanej społeczności, może to być taki przypadek.

Nieuczciwe firmy posługują się też często **różnymi socjotechnikami**, ale to już temat na odrębny artykuł.

BEZPIECZNE ZAKUPY TO TEŻ BEZPIECZNE PŁATNOŚCI

Bezpieczna płatność to nie tylko kwestia konkretnego zakupu. Firma w której kupujesz może być całkowicie uczciwa, ale może także być ofiarą tzw. cyberataków.

Zakupy w online bez oszustw

Dlatego ważne jest żeby sprawdzać procedurę płatności, nawet wtedy, gdy sam sklep wydaje Ci się być uczciwy. Na szczęście, nie musisz mieć bardzo rozbudowanej wiedzy informatycznej, wystarczy przestrzegać podstawowych reguł bezpieczeństwa, a płatności online okażą się dla nas nie tylko wygodne, ale również bezproblemowe.

Kupuj tylko na zaufanych stronach. Sprawdź, czy mają certyfikat SSL (protokół szyfrujący, kłódka w pasku adresu przeglądarki).

Jeżeli płacisz kartą, zwracaj uwagę na certyfikaty bezpieczeństwa, nie podawaj w mailu czy podczas rozmowy przez telefon nieznanej osobie numeru karty i numeru CCV2.

Jeśli płacisz e-przelewem upewnij się, że przekierowanie jest na stronę banku oraz że jest to prawdziwa strona (certyfikat, SSL, poprawnie wyglądający adres).

Dokonuj **płatności tylko na zaufanych urządzeniach** z oprogramowaniem antywirusowym – nie loguj się na swoje konta bankowe i nie po-dawaj danych do płatności, kiedy korzystasz z kafejek internetowych lub ogólnodostępnych darmowych sieci, np. w centrach handlowych.

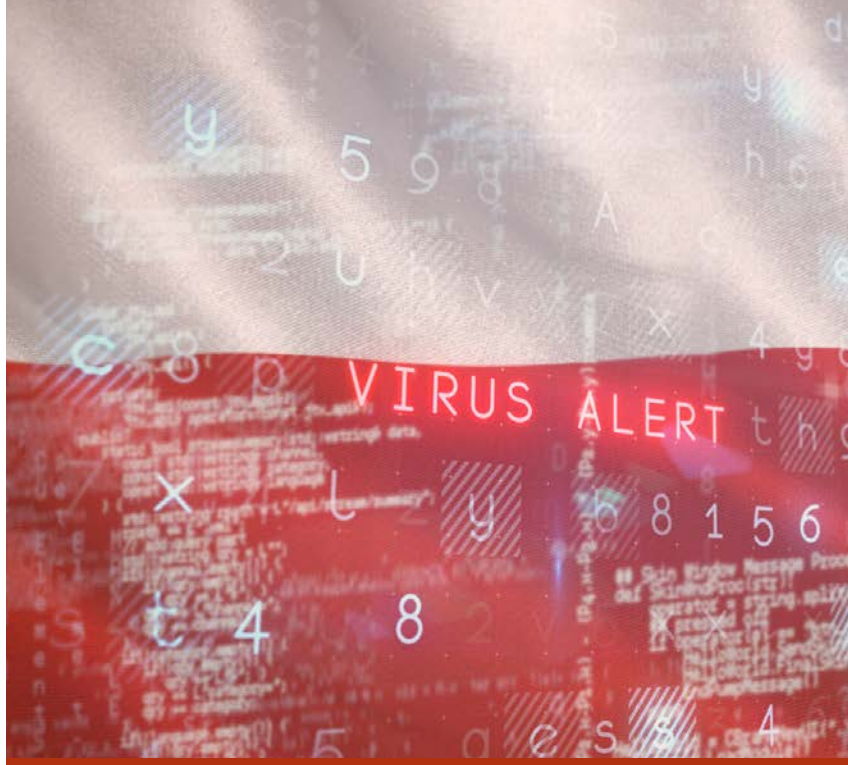
OBSŁUGA PRAWNA E-COMMERCE

WWW.RZETELNYREGULAMIN.PL

SECURITYMAGAZINE.PL

POLSKA 9. NAJBARDZIEJ NARAŻONYM NA CYBERATAKI KRAJEM W UE?

Redakcja
SECURITY MAGAZINE



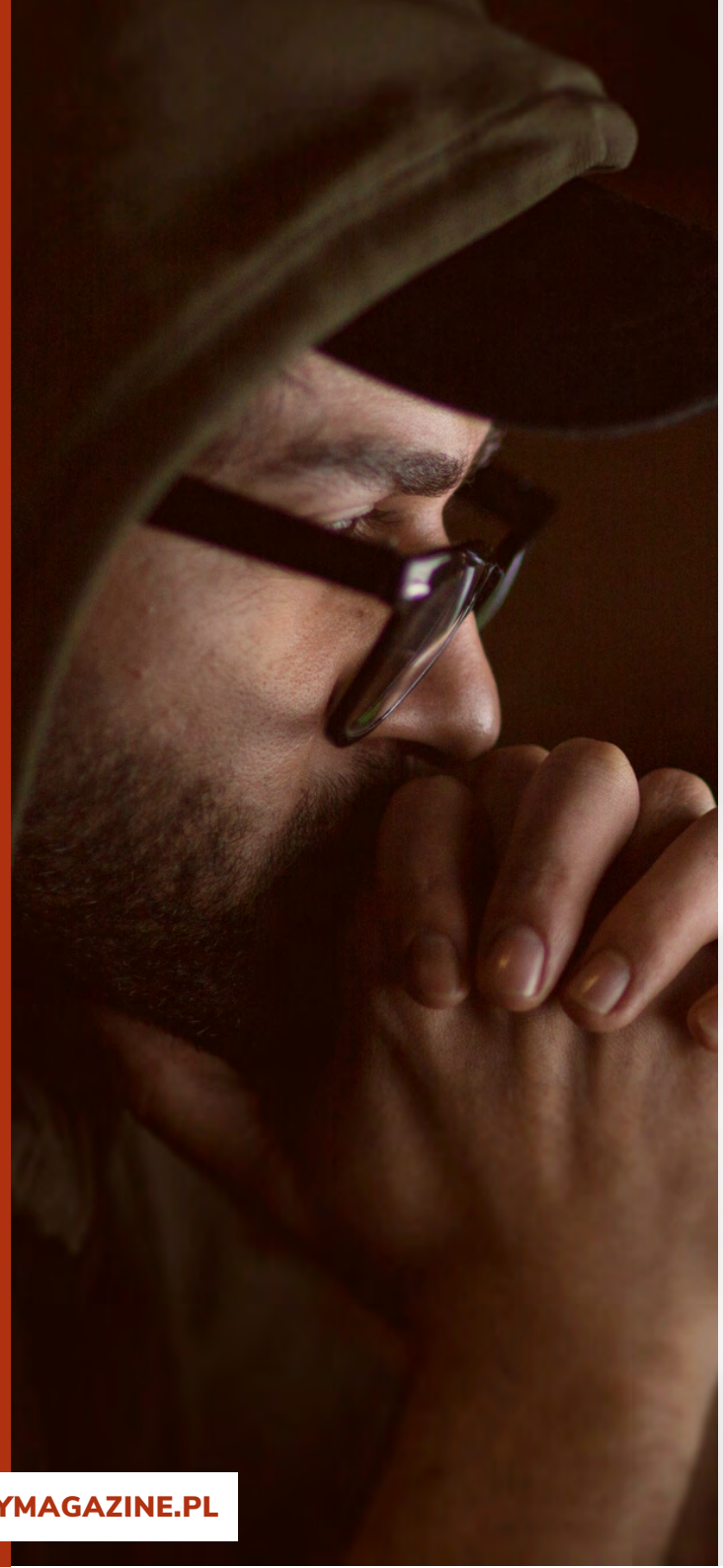
Częstotliwość cyberataków w Polsce się zwiększa. Obecnie jesteśmy narażeni na cyberataki bardziej niż kiedykolwiek. I tyczy się to zarówno sektora prywatnego, jak i publicznego. Co mówią raporty i publikacje o cyberprzestępczości w Polsce?

ZAGROŻENIE CYBERATAKAMI ZWIĘKSZA SIĘ

Jeszcze w 2020 roku, według ekspertów Specops Software, Polska była na 15. miejscu pod względem zagrożenia cyberatakami w Europie. Wówczas to 1. pozycja przypadła Niderlandom (Holandii), 2. Bułgarii, 3. Białorusi, a 4. Ukrainie. Już rok później Polska znalazła się na 9. miejscu w Unii Europejskiej, a w Europie na 13 – tak wskazuje **Global Threat Index Map**, opracowany przez spółkę Check Point. Wówczas zagrożenie cyberatakiem w Polsce oszacowano na 34,9%, co dało nam 69. pozycję wśród wszystkich przebadanych państw.

Jednak w 2022 roku wynik ten wzrósł do 37,5%. Z tego powodu przed nami znalazło się 18 europejskich państw, które były mniej narażone od nas na cyberataki. Również według Check Point polskie przedsiębiorstwa są atakowane średnio **938 razy** w tygodniu. Poważnym zagrożeniem dla naszego kraju są, rzecz jasna, rosyjscy hakerzy, którzy niejednokrotnie otwarcie zadeklarowali odwet na naszym kraju za wspieranie Ukrainy. Choć owym grupom nie zawsze to wychodzi.

Przykładem jest wspierana przez Kreml grupa Killnet znana z **ataków DoS i DDoS**, której lider odgrażał się naszemu państwu niejednokrotnie. Pod koniec marca rosyjscy hakerzy zaatakowali m.in. **Polską Agencję Inwestycji i Handlu (PAIH)**, której dane miały być rozpowszechniane przez cyberprzestępców na Telegramie. PAIH dla serwisu zaufanatrzeciastrona.pl skomentowała sprawę i stwierdziła, że nie doszło do włamania na jej serwery czy do systemu CMS, a pobrane zostały jedynie duże ilości ogólnodostępnych plików.



Eksperci ze wspomnianego wcześniej portalu przeanalizowali udostępnione pliki i okazało się, że spora część z nich faktycznie była ogólnodostępnymi informacjami. Rosjanom udało się przechwycić także kilka maili czy mało istotnych plików w formacie .pdf. Nie było tam jednak nic szczególnie istotnego. Zarówno eksperci zaufanatrzeciastrona.pl, jak i Check Point podkreślają, że akurat ta grupa hakerów, tj. Killnet bardziej niż faktycznym hakingiem, interesuje się budowaniem własnej marki.

Potwierdzałby to też lipcowy atak tych cyberprzestępców na polską policję. Przez kilka godzin strony internetowe niektórych komend wojewódzkich nie działały, a to za sprawą ataków DDoS, jakich dopuścili się Rosjanie. Jednak poza chwilową przerwą w funkcjonowaniu stron – nic szczególnego się nie stało. Nie oznacza to jednak, że należy rosyjskie czy nawet krajowe zagrożenie ignorować – absolutnie. Cyberprzestępczość będzie w zasadzie tylko się zwiększać.

POLSKA NAJBARDZIEJ NARAŻONA NA ATAKI Z WYKORZYSTANIEM MALWARE

Nasz kraj w zasadzie nie odbiega od innych pod względem wykorzystania poszczególnych metod czy oprogramowań do cyberprzestępczości. Według danych Check Point, najczęściej wykorzystywanymi malware'ami u nas są Emotet i Formbook, a także Snake Keylogger. Ten ostatni jest stosunkowo „świeży" i szybko zyskujący na popularności. Jeszcze w maju 2022 roku był 8. najczęściej wykorzystywanym malwarem, ale w czerwcu znalazł się na 3. pozycji.

Snake Keyloggera rozpowszechnia się za pomocą maili zawierających załączniki do dokumentów o rozszerzeniu .docx, będącymi najczęściej prośbami o wycenę.

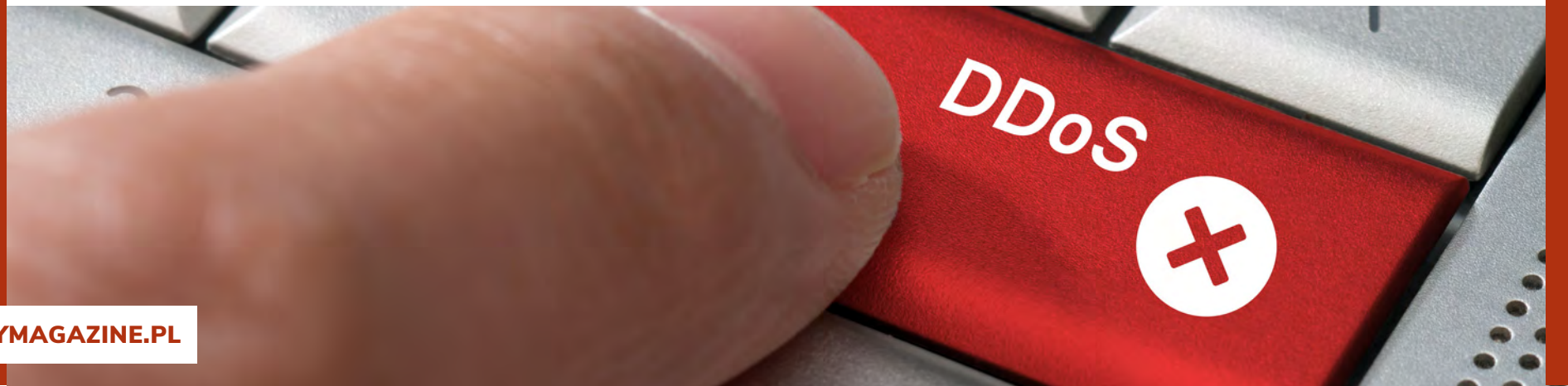
Dane Check Point pokazują nam też, kim najczęściej są cyberprzestępcy. Co prawda, nie mamy informacji bezpośrednio dotyczących Polski, a dla całego regionu EMEA (Europa, Bliski Wschód i Afryka), ale już one same sporo nam mówią.

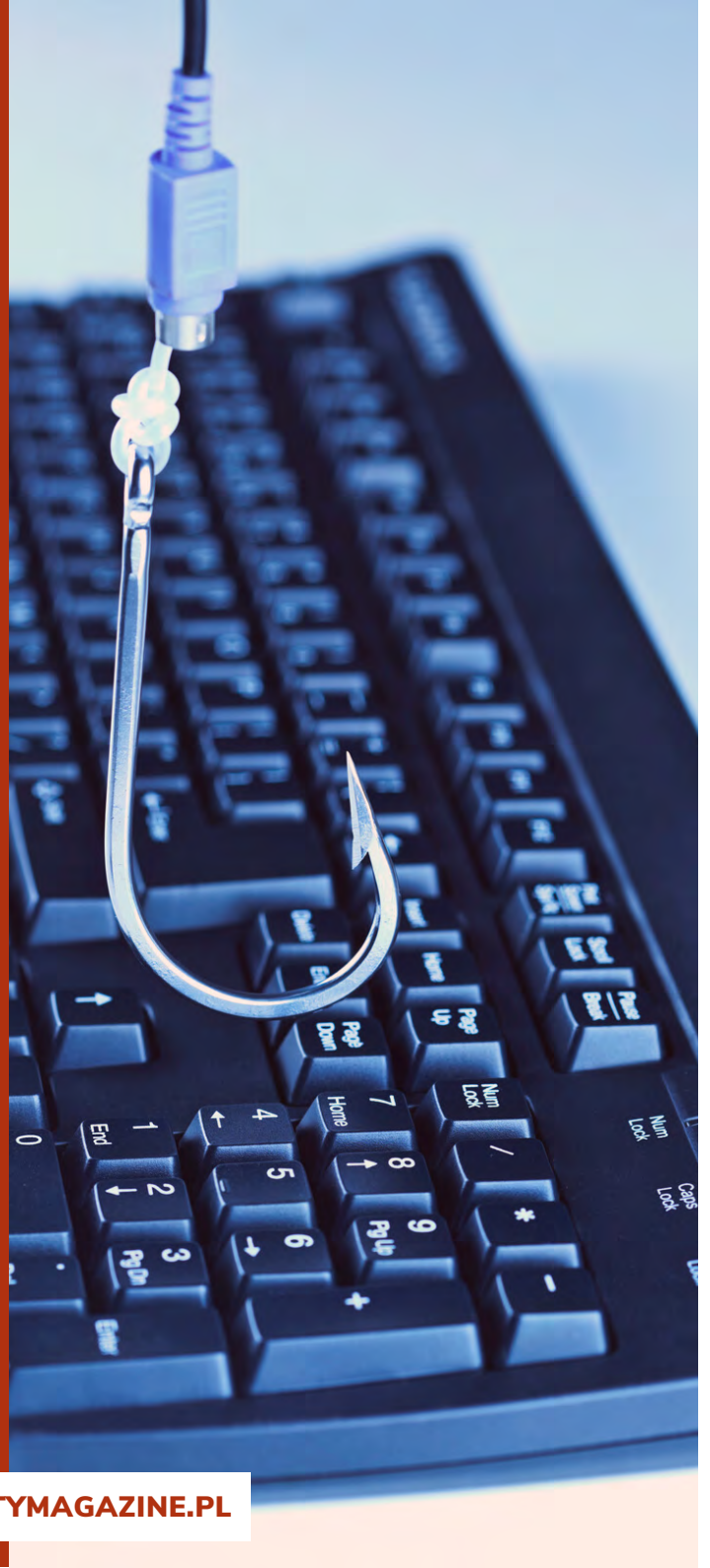
Za 30% ataków w regionie EMEA odpowiadają hakerzy wykorzystujący botnet, czyli sieci komputerów zainfekowane złośliwym oprogramowaniem. Najczęściej służą one do przeprowadzania ataków DDoS – niejednokrotnie bez wiedzy właścicieli tych urządzeń. **23% hakerów to tzw. złodzieje informacji, którzy wykradają dane z firm, instytucji czy od osób prywatnych. Kolejne 19% to górnicy kryptowalut, którzy infekują nasze urządzenia, by te posłużyły im do wykopywania cyfrowych aktywów.**

Wynik ex aequo uzyskali też cyberprzestępcy skupiający się na atakowaniu bankowości internetowej. Natomiast 14% stanowią hakerzy infekujący czy zakłócający działanie aplikacji mobilnych, a 8% do swoich ataków wykorzystuje ransomware. Co za tym idzie – blokuje dostęp do urządzeń IoT, IIoT (przemysłowy internet rzeczy), komputerów lub smartfonów i żąda haraczu za ich odblokowanie.

JAKICH CYBERPRZESTĘPSTW POLSKIE FIRMY OBAWIAJĄ SIĘ NAJBARDZIEJ?

Z danych raportu „Barometr cyberbezpieczeństwa. Ochrona cyfrowej tożsamości" przygotowanego przez KPMG Polska dowiadujemy się, jakich cyberzagrożeń polskie przedsiębiorstwa obawiają się najbardziej.





Autorzy badania poprosili respondentów o ocenienie na skali od zera do pięciu poszczególne zagrożenia. Okazuje się, że najczęściej **polscy przedsiębiorcy boją się phishingu** (32% oceniło to zagrożenie na cztery lub pięć pkt) czy **wycieku danych za pośrednictwem malware** (analogicznie 31%).

Krajowe firmy obawiają się również tzw. APT (zaawansowane trwałe zagrożenie, czyli atak konkretnego państwa lub grupy wspieranej przez jakiś kraj na dane przedsiębiorstwo czy instytucję), jak i kradzieży danych przez pracowników. Te zagrożenia uzyskały kolejno 29% i 30%. Pierwszy przypadek jest całkowicie uzasadniony w związku z wojną w Ukrainie. Jednak o kradzieży danych przez pracowników – czy to byłych, czy obecnych – nie słyszy się aż tak często.

Znacznie powszechniejszym zagrożeniem są ataki DoS/DDoS, przed którymi lęk zadeklarowało jedynie 17% ankietowanych (tj. tyle respondentów oceniło tę metodę na cztery punkty. Nikt nie przyznał mu maksymalnych pięciu). To samo tyczy się ataków ransomware, które jedynie przez 20% przedsiębiorstw zostały ocenione jako poważne.

Jednak zatrważająco często różnego rodzaju cyberzagrożenia przez wiele firm oceniane były na dwa punkty czy mniej. Przykładowe ryzyko ataku DDoS aż przez 30% respondentów zostało ocenione na 2 punkty, a przez kolejne 25% na zero! Jest to o tyle absurdalne, że z raportu dowiadujemy się, iż w 2021 roku

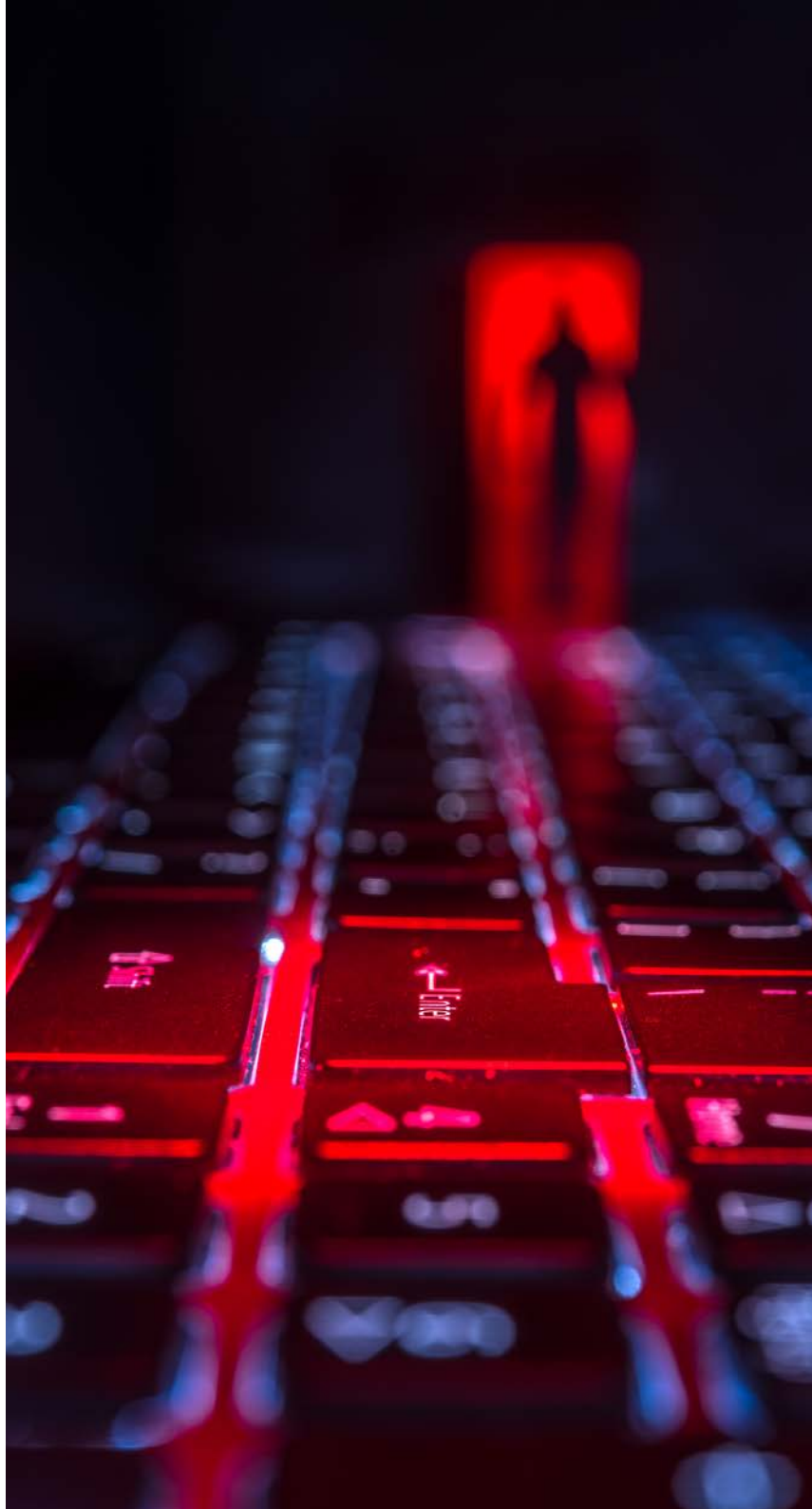
69% firm w Polsce odnotowało przynajmniej jeden incydent związany z cyberbezpieczeństwem. I to o 5 punktów procentowych więcej niż w 2020 r.

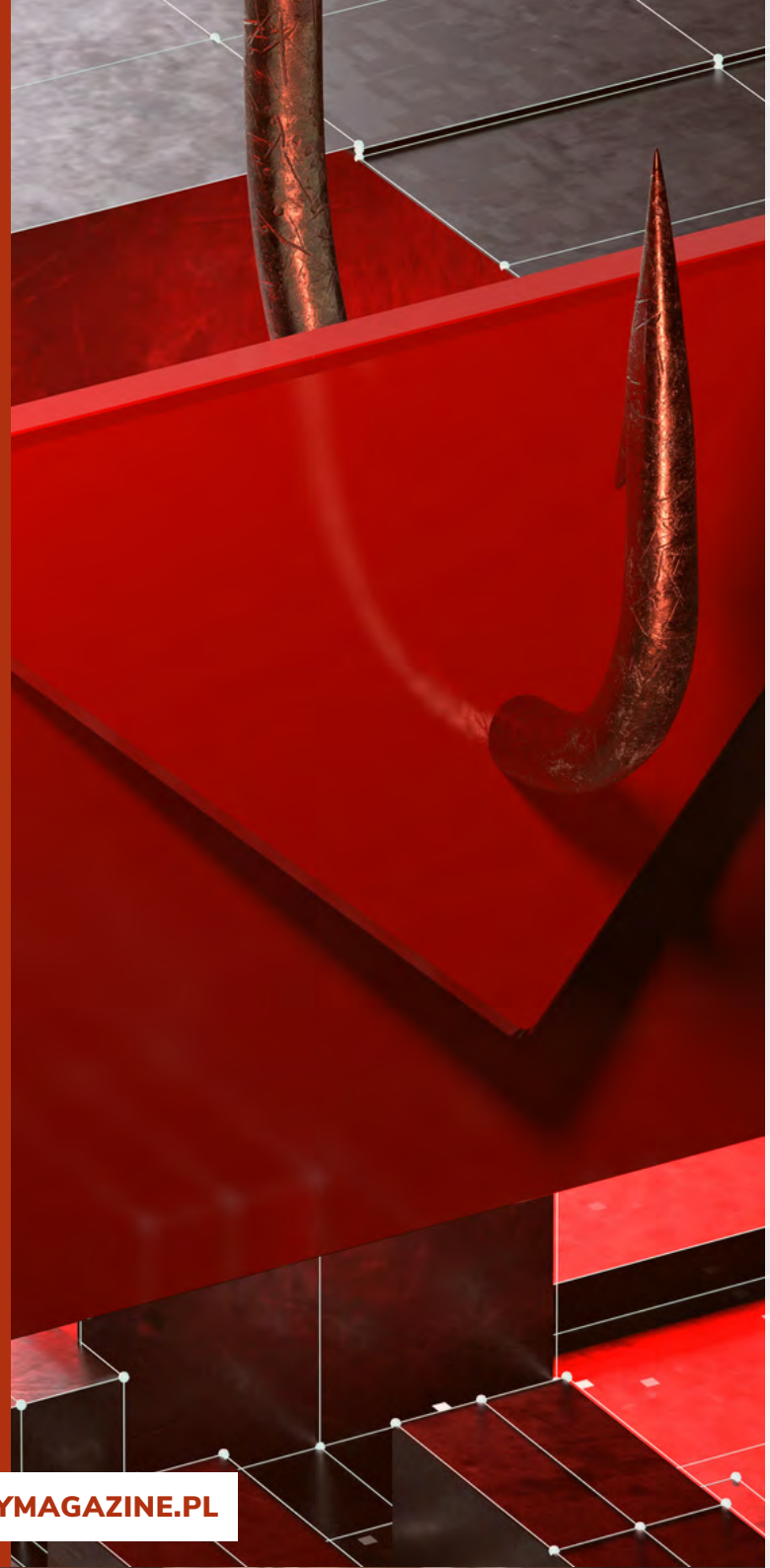
KTO, WEDŁUG POLSKICH PRZEDSIĘBIORCÓW, STANOWI NAJWIĘKSZE ZAGROŻENIE?

Autorzy przytaczanego tu raportu, tj. „Barometru cyberbezpieczeństwa", zapytali również, kto stanowi największe zagrożenie dla organizacji (w formie ankiety wielokrotnego wyboru). Najczęstszą udzielaną odpowiedzią były zorganizowane grupy cyberprzestępcze (69%). Na drugim miejscu znaleźli się pojedynczy hakerzy (58%), a na trzecim cyberterroryści (50%).

Czwartą grupę stanowią niezadowoleni lub podkupieni pracownicy (42%), a piątą grupy wspierane przez obce państwa (27%). Ostatnie pozycje zajęli script kiddies (23%), czyli tzw. crackerzy, którzy wykorzystują głównie oprogramowanie stworzone przez bardziej doświadczone osoby oraz haktywiści (15%) – do najsłynniejszych zaliczają się, chociażby Anonymous.

Dane raportu pokazują nam też, jak zmienia się perspektywa przedsiębiorców na te poszczególne grupy. Jeszcze w 2019 r. najczęściej wskazywanymi zagrożeniami byli pojedynczy hakerzy (84%). Dziś ich rola znacząco zmalała głównie na rzecz cyberterrorystów i zorganizowanych grup cyberprzestępczych.





Zmniejszyło się także postrzeganie haktywistów jako potencjalnego zagrożenia. W 2018 r. (najstarsze dane raportu sięgają właśnie tego okresu) aż według 30% respondentów stanowili oni zagrożenie. To spadek w ciągu czterech lat o 15 p. proc., choć najniższy wynik haktywiści uzyskali w 2019 r. (12%).

Prawdopodobnie to negatywne nastawienie mogło wzrosnąć ze względu na ruchy Anonymous. Owszem – pomagają oni Ukrainie – ale też przecież atakowali prywatne podmioty, które nieszczególnie charakteryzowało solidaryzowanie się z tym państwem po rosyjskiej agresji (abstrahując od tego, czy słusznie, czy nie). Mam tu na myśli np. grupę Nestle. Z tego powodu część przedsiębiorców mogła obawiać się znalezienia na celowniku takich organizacji.

Wojna w Ukrainie wpłynęła też mocno na postrzeganie grup jak wymieniany tutaj na początku Killnet. Do 2021 r. ocena zagrożenia ze strony organizacji wspieranych przez obce państwa zmalała z 33% do 19%. Jednak już w 2022 r. widzimy wzrost o 8 p. proc., co jest jak najbardziej uzasadnione.

Reasumując – praktycznie wszystkie raporty i publikacje wskazują na to, że zagrożenie cyberprzestępczością w Polsce się zwiększyło. Widać to zarówno po twardych danych, tj. wzrostem natężenia cyberataków, jak i wśród nastrojów prywatnego czy publicznego sektora. Polskie firmy i instytucje są narażone na ataki ze strony zarówno rodzimych, jak i obcych hakerów. Czy to niezależnych, czy należących do zorganizowanych grup przestępczych, czy mniej lub bardziej wspieranych przez inne państwa. Polski biznes musi być przygotowany na wyzwania, jakie wiążą się z hakerów, crackerów i innych cyberprzestępców, bo to z pewnością nie zmaleje.


Organizujesz wydarzenie związane
z bezpieczeństwem w firmie
lub nowymi technologiami?
Sprawdź ofertę
PATRONATU
MEDIALNEGO
SECURITY MAGAZINE
Napisz do nas:
redakcja@securitymagazine.pl

EKSPERCI WYDANIA

RENATA DAVIDSON
Founder & CEO
Davidson Consulting

Ekspertka w dziedzinie zarządzania ciągłością działania, ryzykiem operacyjnym i zgodnością. ISO22301 Master. Ekspertka techniczna Polskiego Centrum Akredytacji w obszarze normy ISO 22301. Wykładowczyni Executive MBA (cyberbezpieczeństwo), organizatorka popularnego cyklu bezpłatnych webinarów #RyzykownyCzwartek.

MICHAŁ ROSIAK
Cybersecurity Expert
CERT Orange Polska

Na co dzień bezpieczniak, hobbystycznie – gadżeciarz. Psycholog z wykształcenia, dziennikarz z doświadczenia, ojciec z wyboru, edukator z powołania. Dumny członek zespołu CERT Orange Polska, współautor m.in. CyberTarczy i Bezpiecznego Startera. Konsekwentnie edukuje internautów w zakresie bezpieczeństwa w internecie – słowem, obrazem i technologiami.

KRIS DURSKI
Founder i dyrektor ds. technologii
Vault Security

Starszy analityk oprogramowania, programista, menedżer z ponad 20-letnim doświadczeniem w developingu i marketingu oprogramowania. Opracował koncepcję spersonalizowanego bezpieczeństwa w celu ochrony zasobów cyfrowych i materialnych. Współtworzył kilka start-upów z branży medycznej, technologii informacyjnej i cyberbezpieczeństwa.

MACIEJ ZYGMUNT
Właściciel
Agencja Bezpieczeństwa
i Detektywistyki

Współzałożyciel Stowarzyszenia Praktycy Compliance, właściciel Agencji Bezpieczeństwa i Detektywistyki, były Naczelnik Wydziału CBŚ, detektyw, wykładowca na Wyższej Szkole Bankowej, Wyższej Szkole Bezpieczeństwa oraz Wyższej Szkole Gospodarki Euroregionalnej.

EKSPERCI WYDANIA

INSP. DR MARIUSZ CIARKA
Rzecznik Prasowy
Komenda Główna Policji

Oficer Policji w stopniu inspektora, doktor nauk prawnych, od 2016 roku rzecznik prasowy Komendanta Głównego Policji. Członek Prezydium Rady Polityki Penitencjarnej III kadencji na lata 2020–2024. Dyrektor Biura Komunikacji Społecznej Komendy Głównej Policji. Redaktor naczelny Gazety Policyjnej i miesięcznika POLICJA997.

CHRISTIAN PUTZ
Country Manager
Vectra AI

Odpowiada za działania firmy w Austrii i Europie Środkowo-Wschodniej. Jego rolą jest wspieranie ekspansji firmy w tym rejonie i rozwijanie jej rynkowej strategii. Od wielu lat pełni kluczowe funkcje wykonawcze w wiodących firmach z branży IT, odpowiadając za działy sprzedaży, rozwoju biznesu czy operacji biznesowych.

MAGDALENA GROCHALA
Wspólniczka
Symetria Public Relations

Wspólniczka w agencji Symetria Public Relations. Od 15 lat specjalizuje się w tematyce nowych technologii. Absolwentka Filologii Polskiej oraz Dziennikarstwa i Komunikacji Społecznej na UJ oraz studiów podyplomowych z zakresu cyberbezpieczeństwa na AGH w Krakowie.

MARIUSZ PROCIEWICZ
CISO
Silky Coders

Absolwent Wydziału Zarządzania Uniwersytety Gdańskiego (kierunek Informatyka). Współtworzył i nadzorował obszary zarządzania ciągłością działania i bezpieczeństwa informacji w instytucjach finansowych. Obecnie pełni funkcję CISO w Silky Coders oraz nadzoruje obszar bezpieczeństwa informacji w LPP SA.

EKSPERCI WYDANIA

DARIUSZ TWORZYDŁO
Ekspert. ds. PR
Uniwersytet Warszawski, EXACTO

Ekspert z zakresu PR, doradza zarządom firm, jest trenerem i konsultantem. Wykonuje ekspertyzy, analizy komunikacji wewnętrznej. Opracowuje strategie PR i marketingu. Profesor Uniwersytetu Warszawskiego. Prezes spółki Exacto. Prezes zarządu Stowarzyszenia Agencji Public Relations. Autor ponad 270 artykułów naukowych i publicystycznych, prac badawczych i książek.

TOMASZ KOWALSKI
CEO i współzałożyciel
Secfense

CEO i współzałożyciel firmy z branży cybersecurity Secfense. Posiada ponad 20-letnie doświadczenie w sprzedaży technologii IT, brał udział w setkach wdrożeń sprzętu i oprogramowania w dużych i średnich firmach z sektora finansowego, telekomunikacyjnego, przemysłowego i wojskowego.

JOANNA GIZGIER
CEO w marce
by Fehu

Związana z branżą IT od ponad 11 lat. Zajmuje się projektowaniem i budowaniem stron internetowych oraz e-sklepów, tworzy layoty w WordPress. Dba o działania SEO. Zajmuje się też identyfikacją wizualną marki. Jest autorką szkoleń: “Twoje miejsce w sieci” czy “Firmowe błędy w poruszaniu się online”.

RAFAŁ STĘPNIEWSKI
Prezes Zarządu
Rzetelna Grupa Sp. z o.o.

Redaktor naczelny serwisu dziennikprawny.pl i Security Magazine. Z branżą e-commerce związany od ponad 15 lat. Manager z 20-letnim doświadczeniem w branżach IT&T i zarządzaniu. Autor wielu publikacji z zakresu prawa e-commerce oraz bezpieczeństwa.

PARTNERZY WYDANIA

KOMENDA GŁÓWNA POLICJI

VECTRA AI

FIRMA ZAJMUJĄCA SIĘ
CYBERBEZPIECZEŃSTWEM
Z SIEDZIBĄ W KALIFORNII

POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY
O BEZPIECZEŃSTWIE FIRM

RZETELNY REGULAMIN

BLOG POŚWIĘCONY
POLSKIEMU E-COMMERCE

POLICJA

VECTRA®

Polityka® Bezpieczeństwa

Rzetelny® Regulamin

ZOBACZ WYDANIA

Wydanie 1/2022

POBIERZ

Wydanie 2/2022

POBIERZ

Wydanie 3/2022

POBIERZ

Wydanie 4/2022

POBIERZ

Wydanie 5/2022

POBIERZ

Wydanie 6/2022

POBIERZ

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

al. Jana Pawła II 61 lok. 212
01-031 Warszawa

KRS 284065
NIP: 524-261-19-51
REGON: 141022624
Kapitał zakładowy: 50.000 zł
Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy
Magazyn wpisany do sądowego Rejestru dzienników i czasopism.

Redaktor Naczelny: Rafał Stępniewski

Redakcja: Monika Świetlińska, Damian Jemioło
Projekt, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL